Part I – Lab Setup Guide

Swapnil Pathak
Amit Malik

www.SecurityXploded.com

Disclaimer

The Content, Demonstration, Source Code and Programs presented here is "AS IS" without any warranty or conditions of any kind. Also the views/ideas/knowledge expressed here are solely of the trainer's only and nothing to do with the company or the organization in which the trainer is currently working.

However in no circumstances neither the trainer nor SecurityXploded is responsible for any damage or loss caused due to use or misuse of the information presented here.

Acknowledgement

- Special thanks to **null** & **Garage4Hackers** community for their extended support and cooperation.
- Thanks to all the trainers who have devoted their precious time and countless hours to make it happen.

Reversing & Malware Analysis Training

This presentation is part of our **Reverse Engineering & Malware Analysis** Training program. Currently it is delivered only during our local meet for FREE of cost.

For complete details of this course, visit our Security Training page.

Who am I #1

Amit Malik (sometimes DouBle_Zer0,DZZ)

- Member SecurityXploded
- Security Researcher @ McAfee Labs
- RE, Exploit Analysis/Development, Malware Analysis
- Email: m.amit30@gmail.com

Who am I #2

Swapnil Pathak

- Member SecurityXploded
- Security Researcher @ McAfee Labs
- RE, Malware Analysis, Network Security
- Email: swapnilpathak101@gmail.com

Course Q&A

- Keep yourself up to date with latest security news
  - http://www.securityphresh.com
- For Q&A, join our mailing list.
  - http://groups.google.com/group/securityxploded

Introduction

- This Guide is specific to our course
- Although it will cover most of the tools and techniques for an analysis environment
- Our main focus is on the famous tools

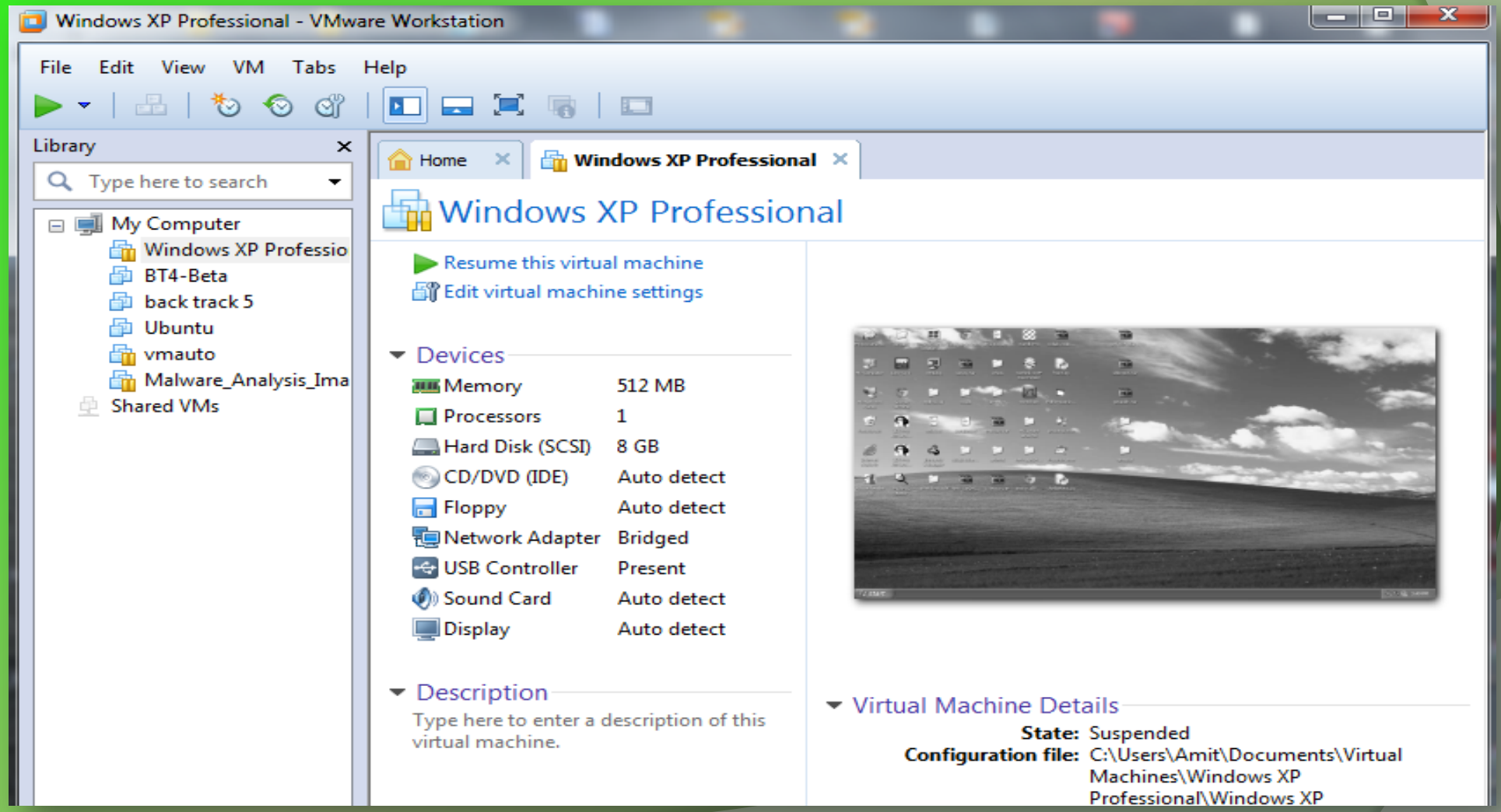
Virtualization

- Run multiple OS on the single hardware at the same time.
- Advanced functionalities like Snapshot, Revert Back, pause etc.
- Automation
- Controlled environment

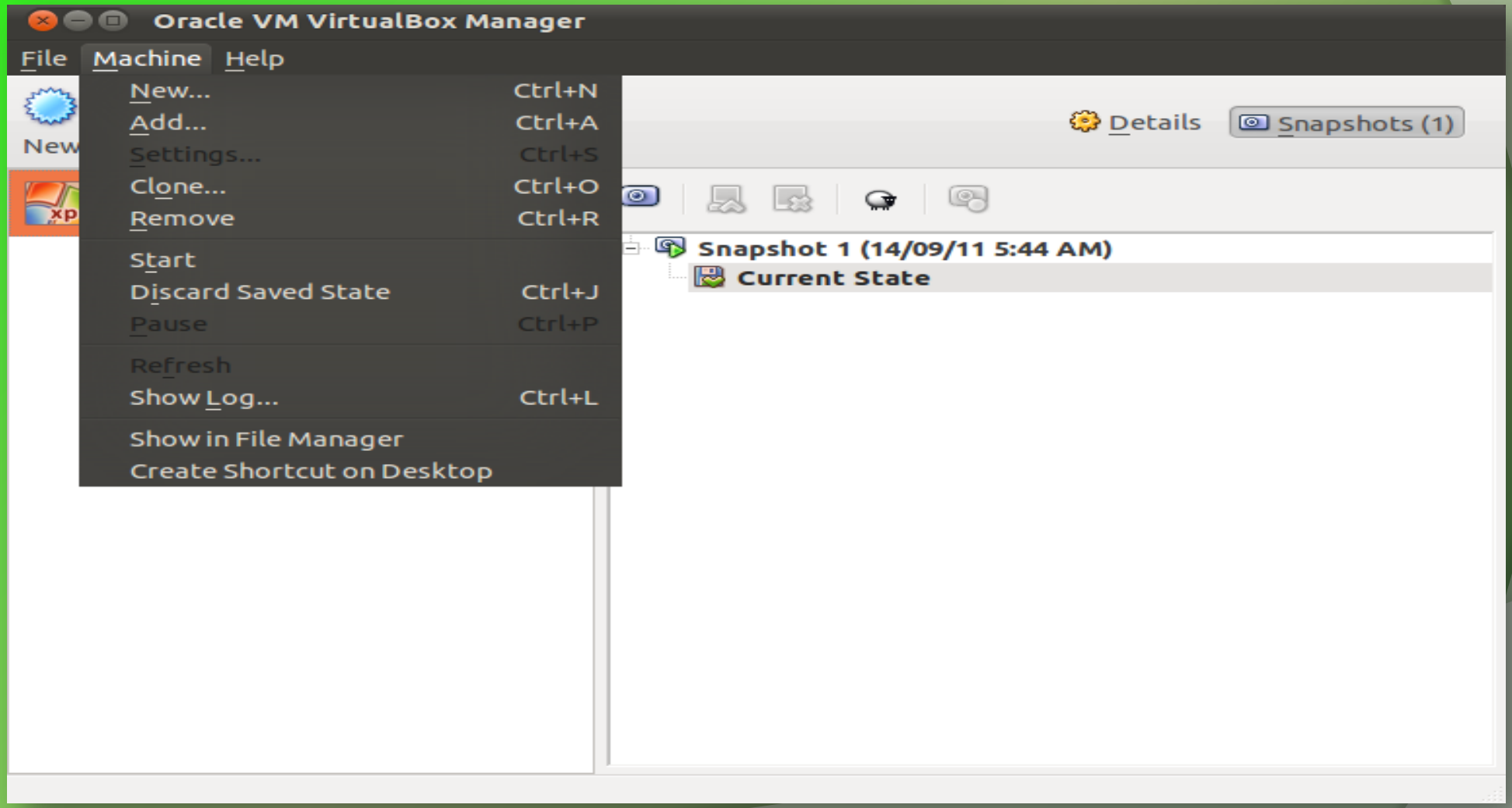
Virtualization Tools

- VmWare (Commercial)
- VirtualBox (Open Source – free)
- Images – XpSp2, XpSp3

VmWare Image



VirtualBox Image



Tools Development

- Compiler/IDE
  - Dev C++ (Free) - preferred
  - Microsoft Visual C++ (Commercial)
- Assemblers
  - MASM (Free) -preferred
  - NASM (Free)
  - Winasm (IDE) (Free)
- Interpreters
  - Python (Free)

Tools Reverse Engg.

- Disassembler:
  - IDA Pro (Download free version)
- Debuggers
  - Ollydbg
  - Immunity Debugger
  - Windbg
  - Pydbg (optional)

Tools Reverse Engg. Cont.

- PE file Format
  - PEview, PEbrowse, LordPE, ImpRec, Peid, ExeScan
- Process Related
  - ProcMon, Process explorer
- Network Related
  - Wireshark, TcpDump, Tshark, TCPView
- File, Registry Related
  - Regshot, filemon, InstallwatchPro, CaptureBat

Tools Reverse Engg. Cont.

- Misc.
  - CFFExplorer, Notepad++, Dependency Walker, Sysinternal tools
- If something additional is required then we will cover that in the respective lecture

Reference

- Complete Reference Guide for Reversing & Malware Analysis Training

Thank You !

www.SecurityXploded.com