Windows Forensics

Dr. Phil Polstra   @ppolstra
PhD, CISSP, CEH   http://philpolstra.com

Certifications:
http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

About Me

- Frequent conference speaker
  - Repeat performances at DEFCON, BlackHat, GrrCON, 44CON, B-sides, ForenSecure, ...
  - BruCON, SecTOR, ShakaCON, ...
- Author
  - ***Hacking and Penetration Testing with Low Power Devices***
  - ***Linux Forensics***
  - ***USB Forensics***
- Associate Professor of Digital Forensics, Bloomsburg University of Pennsylvania
- Programming from age 8 (in Assembly at 10)
- Hacking hardware from age 12
- Aviator and plane builder with a dozen ratings

Course Contents

Live Response
- Human interactions
- Creating a live response kit
- Transporting data across a network
- Collecting volatile data
- Determining if dead analysis is justified
- Dumping RAM

Course Contents (cont.)

Acquiring filesystem images

- Using dd
- Using dcfldd & dc3dd
- Write blocking
  - Software blockers
    - Udev rules
    - Forensic Linux distros
  - Hardware blockers

Course Contents (cont.)

Analyzing filesystems
- Mounting image files
    - Finding the strange
    - Searching tools
    - Authentication related files
    - Recovering deleted files
    - Finding hidden information

Course Contents (cont.)

The Sleuth Kit (TSK) and Autopsy
- Volume information
- Filesystem information
- FAT 12/16/32
- NTFS
- Directory entries
- Constructing timelines

Course Contents (cont.)

Timeline Analysis

- When was system installed, upgraded, booted, etc.
- Newly created files (malware)
- Changed files (trojans)
- Files in the wrong place (exfiltration)

Course Contents (cont.)

Digging deeper into Windows filesystems

- Disk editors
  - Active@ Disk Editor
  - Autopsy
- FAT 12/16/32
- NTFS
- Searching unallocated space

Network forensics

- Using snort on packet captures
- Using tcpstat
- Seperating conversations with tcpflow
- Tracing backdoors with tcpflow

Course Contents (cont.)

File forensics

- Using file signatures
- Searching through swap space
- Web browsing reconstruction
  - Cookies
  - Search history
  - Browser caches

Unknown files
  - Comparing hashes to know values
  - File and strings commands
- Log files
- Recycle bin
- Prefetch files
- Alternate data streams

©SecurityTube.net

Course Contents (cont.)

Registry forensics

- RegRipper
- Python
- System information
- Autostart programs
- USB Devices
- User info

- Past & present mounted devices
- User activity
- System restore points

Course Contents (cont.)

Memory Forensics
- Retrieving process information
- Windows objects
- Looking for malware
- Event logs
- Registry in memory
- Reconstructing network artifacts
- Windows services
- Windows GUI
- Filesystems in memory
- Detecting kernel rootkits
- Creating timelines

Course Contents (cont.)

Reversing Windows
Malware

- Windows executables
  - Headers
  - Imports
  - Exports
  - Resources
  - Obfuscation
  - Dynamic linking

- Command line analysis
  tools
  - strings

- Running malware
  (carefully)
  - Virtual machine setup
  - Capturing network
    traffic
  - Leveraging debuggers

Course Contents (cont.)

Writing the reports

- Autopsy

- Dradis

- OpenOffice

Overall Goals

- Leverage open source (or at least free) software

- Hands on practical exercises and demos throughout

- Provide the most comprehensive Windows forensics course available