Linux Forensics

Dr. Phil Polstra

PhD, CISSP, CEH

@ppolstra

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***
  - Two new books planned for 2015
- 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
- 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
- Inodes
- 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 Linux filesystems

- Disk editors
  - Active@ Disk Editor
  - Autopsy
- ExtX
- Other Linux filesystems
- Searching unallocated space

Course Contents (cont.)

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
- Viewing symbols with nm
- Reading ELF files
- objdump
- gdb

Course Contents (cont.)

Memory Forensics

- Volatility Profiles
- Retrieving process information
- Recovering command line arguments
- Rebuilding environment variables
- Listing open files
- Retrieving bash information
- Reconstructing network artifacts
- Kernel information
- Volatile file system information
- Detecting user mode rootkits
- Detecting kernel rootkits

Course Contents (cont.)

Reversing Linux Malware

- Digging deeper into ELF
  - Headers
  - Sections
  - Strings
  - Symbol tables
  - Program headers
  - Program loading
  - Dynamic linking
- Command line analysis tools
  - strings
  - strace
  - ltrace
- Running malware (carefully)
  - Virtual machine setup
  - Capturing network traffic
  - Leveraging gdb

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 Linux forensics course available