

Linux Forensics BY Hal Pomeranz

(In Canberra)

(In Melbourne)

3-6 Apr 2023

11-14 Apr 2023



1300 55 33 24 | www.cdfs.com.au





About Linux

Linux is everywhere-- running in the cloud, on cell phones, and in embedded devices that make up the "Internet of Things". Often neglected by their owners, vulnerable Linux systems are low-hanging fruit for attackers wishing to create powerful botnets or mine cryptocurrencies. Ransomware type attacks may target Linux-based database systems and other important infrastructure.

As attacks against Linux become more and more common, there is an increasing demand for skilled Linux investigators. But even experienced forensics professionals may lack sufficient background to properly conduct Linux investigations. Linux is its own particular religion and requires dedicated study and practice to become comfortable.

This four-day, hands-on course is a quick start into the world of Linux forensics. Learn how to use memory forensics to rapidly triage systems and spot attacker malware and rootkits. Learn where the most critical on-disk artifacts live and how they can help further an investigation. Rapidly process Linux logs and build a clearer picture of what happened on the system.

INSTRUCTOR

Hal **Pomeranz**



is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft, to employee sabotage, to organized cybercrime and malicious software infrastructures. He has spent more than thirty years providing pragmatic Information Technology and Security solutions for some of the world's largest commercial, government, and academic institutions.



KEY TAKEAWAYS











Linux live collection and analysis

Rapid triage for key Linux artifacts

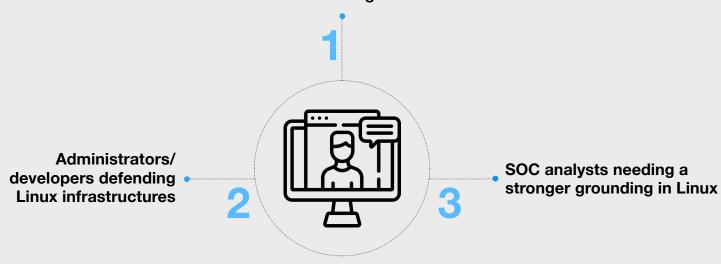
Accessing complex Linux disk geometries

Linux log analysis

File system internals and deleted data recovery

WHO SHOULD TAKE THIS COURSE

Experienced forensic professionals wanting to expand their Linux knowledge





AUDIENCE SKILL LEVEL

This course is an introduction to Linux forensics, but not an introduction to forensics. The course assumes at least some knowledge of digital forensic methods, such as evidence acquisition. This course is heavily command-line driven, so basic familiarity with the Linux command-line is helpful.

WHAT STUDENTS WILL BE PROVIDED WITH



course slides and author notes in PDF form



lab exercises and virtual machine, and sample forensic images

PRICE

\$6000 per person ex GST



* Vouchers can only be used for courses delivered by CDFS at our training facility or via Virtual Instructor-Led Training.



Day One – Memory Forensics

1. Memory Forensics - Acquisition

Why memory forensics?
Acquisition tools and scenarios
Building memory analysis profiles
Automation

LAB: Memory Capture and Volatility Profile Creation

2. Memory Forensics - Analysis

Kernel messages

Processes

Networking

Command history

File system

LAB: What's In Memory?

3. Memory Forensics - Case Study

Spotting the rootkit module in memory
Looking for hooks
Using indicators of compromise

LAB: Rootkit Investigation

4. Memory Forensics - With bulk-extractor

- Running bulk-extractor
- Useful artifacts
- Examining extracted PCAPs

LAB: No profile? No problem!



Day Two – Linux Live Capture

1. Live Capture with UAC

Memory forensics is great but... Configuring and running UAC Deployment options

LAB: : Collecting data with UAC

2. Live Analysis and Triage - File System

Standard directory layout, ownerships, and permissions Spotting malicious executables
Deeper dives with /proc

LAB: Too much evil!

3. Live Analysis and Triage – Processes

The process hierarchy
Typical process ownership
Suspicious process anti-patterns

LAB: : Even more evil!

4. Live Analysis and Triage – Users and Groups

Superuser, application users, and regular users
 Processes and users anti-patterns
 User back doors

LAB: Find the back door(s)





Day Three - Linux Disk Analysis

1. **Disk Acquisition and Access**

Acquisition scenarios and tools Complex disk geometries Setup and teardown walk-throughs

LAB: : Disk Image Mounting Challenge

2. **Rapid Disk Triage**

Critical system directories

System profiling

Common back doors

Persistent malware

Finding recently modified files

LAB: Disk Triage

3. **Timeline Analysis**

Why timeline analysis? Unix timestamps

Generating timeline

LAB: : Timeline Analysis

4. **Linux Log Basics**

User access (wtmp, btmp, lastlog) Understanding where logs live via syslog.conf **Linux Syslog log format** Which logs are most useful?

LAB: Using Logs to Enhance Timeline Analysis

5. **Digging Deeper Into Logs**

Web server logs

Kernel logging with auditd

Searching kernel audit logs

Keystroke logging

LAB: Web Server Compromise Logs





Day Four - Digging Deeper

1. User Artifacts:

Bash_history SSH artifacts, inbound and outbound Editing history Recently opened file history Web history

LAB: : Post-Exploitation Activity

2. EXT File System Analysis:

Key data structures and layout Tools for examining EXT Reverse-engineering EXT case study

LAB: Recover Deleted Exploit

3. XFS File System Analysis:

Key data structures and layout Tools for examining XFS Data recovery methods

LAB: : XFS file system walkthrough

4. Web Compromise - Case Study

Spotting patterns of activity
Separating multiple actors
Matching logs to system activity
Pivoting to find further information

LAB: Choose your own adventure(s)