Linux Incident Response and Forensics Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The modern enterprise relies heavily on Linux-based systems to power critical infrastructure, from web servers and databases to cloud environments and IoT devices. This ubiquity makes Linux Security a prime target for sophisticated threat actors, including Advanced Persistent Threats (APTs) and organized cybercrime syndicates. The ability to perform rapid, effective Digital Forensics and Incident Response (DFIR) on these systems is no longer a niche skill it is a mandatory and high-demand competency for every Cybersecurity professional. The gap in expertise is evident: many security teams are skilled in Windows or network security but lack the deep-dive, command-line-centric proficiency required to properly handle a Linux breach. Linux Incident Response and Forensics Training Course provides the hands-on experience and forensic methodology necessary to bridge that gap, ensuring that critical evidence is preserved, attacker Tactics, Techniques, and Procedures (TTPs) are fully uncovered, and system integrity is restored swiftly.

This intensive training is engineered to equip security practitioners with advanced Linux forensic analysis skills, focusing on live-system triage, memory forensics, and threat hunting. You will master open-source DFIR tools and advanced Bash scripting to effectively investigate a range of complex incidents, including web shell compromise, rootkits, and ransomware attacks on Linux servers. By adopting a structured incident response framework and applying practical, real-world case studies, participants will gain the confidence to lead complex Linux investigations from initial detection to final remediation and reporting, thereby dramatically improving their organization's cyber defense posture and minimizing the impact of the next security incident.

Programme Curriculum

Linux Incident Response and Forensics Training Course

Introduction

The modern enterprise relies heavily on Linux-based systems to power critical infrastructure, from web servers and databases to cloud environments and IoT devices. This ubiquity makes Linux Security a prime target for sophisticated threat actors, including Advanced Persistent Threats (APTs) and organized cybercrime syndicates. The ability to perform rapid, effective Digital Forensics and Incident Response (DFIR) on these systems is no longer a niche skill it is a mandatory and high-demand competency for every Cybersecurity professional. The gap in expertise is evident: many security teams are skilled in Windows or network security but lack the deep-dive, command-line-centric proficiency required to properly handle a Linux breach. Linux Incident Response and Forensics Training Course provides the hands-on experience and forensic methodology necessary to bridge that gap, ensuring that critical evidence is preserved, attacker Tactics, Techniques, and Procedures (TTPs) are fully uncovered, and system integrity is restored swiftly.

This intensive training is engineered to equip security practitioners with advanced Linux forensic analysis skills, focusing on live-system triage, memory forensics, and threat hunting. You will master open-source DFIR tools and advanced Bash scripting to effectively investigate a range of complex incidents, including web shell compromise, rootkits, and ransomware attacks on Linux servers. By adopting a structured incident response framework and applying practical, real-world case studies, participants will gain the confidence to lead complex Linux investigations from initial detection to final remediation and reporting, thereby dramatically improving their organization's cyber defense posture and minimizing the impact of the next security incident.

Course Duration

5 days

Course Objectives

1. Master the Linux DFIR methodology and legal Chain of Custody protocols.
2. Perform Live-System Triage on compromised Linux hosts, prioritizing volatile data.
3. Utilize Advanced Forensics Tools for deep-dive analysis.
4. Conduct comprehensive Linux Memory Forensics to uncover hidden process injection and malware artifacts.
5. Analyze Ext4/XFS File Systems for deleted files, slack space, and anti-forensics techniques.
6. Investigate complex Web Shell Compromise scenarios on common Linux web servers
7. Identify and analyze Persistence Mechanisms and Linux Rootkits used by sophisticated adversaries.
8. Perform System Log Analysis to reconstruct the attacker's Kill Chain.
9. Develop Endpoint Threat Hunting strategies for proactive detection of unknown malicious activity.
10. Reverse-engineer Attacker TTPs using MITRE ATT&CK Framework mapping for Linux environments.
11. Collect and analyze network evidence via Network Forensics to trace lateral movement.
12. Create Super Timelines of system activity to correlate disparate events and build a cohesive narrative.
13. Generate professional, legally sound Forensic Investigation Reports for management and legal teams.

Target Audience

1. Incident Response Team Members.
2. Digital Forensics Analysts.
3. SOC Analysts.
4. Cyber Threat Hunters.
5. Linux System Administrators.
6. Security Engineers/Architects.
7. Penetration Testers/Red Team.

8. IT/Security Managers.

Course Modules

Module 1: DFIR Fundamentals and Live Triage

- Linux Incident Response Lifecycle
- Legal and Ethical Considerations
- Establishing the Forensic Workstation.
- Volatile Data Acquisition using LiME and native tools.
- Case Study: Responding to a Zero-Day Exploit on a live Apache server, focusing on safe collection of volatile data before shutdown.

Module 2: Filesystem and Disk Acquisition

- Linux File System Internals
- Disk Imaging Techniques
- Analyzing Timestamps and anti-forensics time manipulation.
- Volume Management and encryption handling for forensic purposes.
- Case Study: Investigating an Insider Threat who deleted critical source code files; techniques for recovering data from unallocated space.

Module 3: System Artifacts and User Activity

- Analyzing User Account Artifacts and suspicious UID/GIDs.
- Reconstructing user activity via Bash History analysis, sudo logs, and TTY records.
- Investigating Persistence Mechanisms
- Analyzing network configuration and evidence of SSH Compromise
- Case Study: Tracing the lateral movement of an attacker who escalated privileges from a low-privilege web user to root using a compromised SSH key.

Module 4: Log and Timeline Analysis

- Deep-dive into System Logs for event correlation.
- Techniques for detecting Log Tampering and log rotation inconsistencies.
- Building a Super Timeline with Plaso/log2timeline to create a unified view of events.
- Focus on Authentication Logs for brute force and login anomalies.
- Case Study: A Web Server Breach investigation where log analysis uncovers a PHP web shell planted months before the main attack.

Module 5: Linux Memory Forensics

- Fundamentals of Memory Analysis and the Linux kernel memory structures.
- Using the Volatility Framework for Linux.
- Extracting command history, network socket information, and environment variables from a memory dump.
- Identifying and locating Malware and Fileless Attacks running solely in memory.
- Case Study: Detecting a sophisticated Linux Rootkit that was only visible in the kernel memory dump, having successfully hidden itself from host-based tools.

Module 6: Network and Application Forensics

- Investigating common Web Server Logs for suspicious requests and POST data
- Analyzing network communication and artifacts to trace Data Exfiltration.
- Forensics of other common services.
- Techniques for analyzing Packet Captures related to the incident using Wireshark.
- Case Study: Uncovering the full scope of a Ransomware Attack on a corporate file server, tracing the command-and-control communication via network logs.

Module 7: Advanced Anti-Forensics and Automation

- Identifying and countering attacker Anti-Forensics techniques
- Introduction to Container and Cloud Forensics
- Developing custom Bash Scripts and Python tools for rapid, repeatable evidence triage.
- Integrating DFIR with Endpoint Detection and Response solutions for at-scale hunting.
- Case Study: Analyzing a system where the attacker attempted to use secure-delete and advanced time manipulation to hide their activity.

Module 8: Reporting and Remediation

- Structuring a Forensic Investigation Report for both technical and executive audiences.
- Developing clear, actionable Indicators of Compromise for immediate defense.
- The Eradication and Recovery phase: ensuring the system is clean and hardened.
- Conducting Lessons Learned and process refinement based on the investigation.
- Case Study: Presenting the final report on a state-sponsored APT intrusion, detailing the full Kill Chain, the evidence collected, and the recommended hardening steps.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com