Linux Security Hardening and Administration 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

Linux Security Hardening and Administration Training Course is designed to equip IT professionals, system administrators, and security specialists with the in-demand skills to secure critical Linux servers against advanced persistent threats (APTs) and zero-day vulnerabilities. It focuses on practical, hands-on implementation of Zero Trust principles, DevSecOps best practices, and compliance mandates like CIS Benchmarks to minimize the attack surface and ensure robust, resilient Linux environments.

Our curriculum goes beyond basic configurations, delving into advanced kernel security, intrusion detection/prevention systems (IDS/IPS), and secure remote access via SSH hardening and multi-factor authentication (MFA). You'll master tools and techniques for vulnerability management, real-time log auditing (SIEM), and managing crucial security modules like SELinux and AppArmor. Completing this course will certify your ability to administer, audit, and fortify high-stakes Linux systems, making you an essential asset in today?ÇÖs cybersecurity landscape and ready to tackle cloud security challenges.

Programme Curriculum

Linux Security Hardening and Administration Training Course

Introduction

Linux Security Hardening and Administration Training Course is designed to equip IT professionals, system administrators, and security specialists with the in-demand skills to secure critical Linux servers against advanced persistent threats (APTs) and zero-day vulnerabilities. It focuses on practical, hands-on implementation of Zero Trust principles, DevSecOps best practices, and compliance mandates like CIS Benchmarks to minimize the attack surface and ensure robust, resilient Linux environments.

Our curriculum goes beyond basic configurations, delving into advanced kernel security, intrusion detection/prevention systems (IDS/IPS), and secure remote access via SSH hardening and multi-factor authentication (MFA). You'll master tools and techniques for vulnerability management, real-time log auditing (SIEM), and managing crucial security modules like SELinux and AppArmor. Completing this course will certify your ability to administer, audit, and fortify high-stakes Linux systems, making you an essential asset in today? ÇÖs cybersecurity landscape and ready to tackle cloud security challenges.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Implement Zero Trust Network Access (ZTNA) principles for Linux environments.
2. Apply CIS Benchmarks and STIG guidelines for server hardening and compliance.
3. Master SELinux and AppArmor for Mandatory Access Control (MAC).
4. Perform Vulnerability Assessment and Penetration Testing (Pen Testing) on Linux systems.
5. Configure Advanced Firewall rules using nftables and iptables.
6. Secure SSH access with Key-Based Authentication and Multi-Factor Authentication (MFA).
7. Manage Pluggable Authentication Modules for robust User Authentication.
8. Deploy File Integrity Monitoring (FIM) solutions for change detection.
9. Analyze system and security logs using SIEM (Security Information and Event Management) concepts.
10. Administer Identity and Access Management (IAM) policies across the Linux estate.
11. Implement Kernel Hardening techniques and manage rebootless patching.
12. Develop an effective Linux Incident Response and Disaster Recovery plan.
13. Automate security configurations using Configuration Management tools.

Target Audience

1. Linux System Administrators.
2. IT Security Analysts.
3. DevOps Engineers.
4. Cybersecurity Professionals.
5. Security Architects.
6. Cloud Engineers.
7. Compliance and Audit Personnel
8. Technical Support Staff.

Course Modules

Module 1: Foundational Linux Administration for Security

- Review of essential command-line tools and secure shell usage.
- Secure file system and partition management best practices.
- System initialization and runlevel management for minimal attack surface.
- Secure package management and repository configuration.
- Managing kernel parameters for security, including sysctl tuning.
- Case Study: Analyzing a breach caused by an unpatched vulnerability in an obsolete, unmanaged package repository.

Module 2: User Authentication and Access Control Hardening

- Implementing strong password policies using PAM
- Configuring and enforcing MFA for all privileged access.
- Securing sudoers and managing delegated administrative privileges.
- Implementing SSH Hardening
- Advanced user and group management, including lifecycle management and privileged access management principles.
- Case Study: The compromise of a major corporation due to a weak, brute-forced root password and lack of MFA on an external SSH gateway.

Module 3: System Hardening and Configuration Management

- Applying CIS Benchmarks for Linux system hardening
- Disabling and removing unnecessary services to minimize the attack surface.
- Securing the bootloader and securing system binaries.
- Utilizing Aide or Tripwire for File Integrity Monitoring.
- Automating hardening procedures using Ansible or Puppet for consistency and scale.
- Case Study: A successful audit defense achieved by automating CIS benchmark compliance across hundreds of servers using an Infrastructure-as-Code tool.

Module 4: Kernel Security and Mandatory Access Control (MAC)

- Understanding and configuring SELinux security policies in enforcing mode.
- Implementing AppArmor profiles for application confinement.
- Deep dive into kernel runtime security parameters and memory protection.
- Implementing rebootless patching solutions for kernel security updates.
- Leveraging Linux Security Modules for advanced security enforcement.
- Case Study: Using SELinux to contain a malware infection, preventing it from escalating privileges and accessing sensitive directories.

Module 5: Network Security and Host-Based Firewall

- In-depth configuration of the nftables and iptables host-based firewalls.
- Implementing TCP Wrappers and securing network services.
- Configuring and securing VPNs and tunneling for remote access.
- Network interface and protocol hardening
- Setting up basic IDS/IPS capabilities on the Linux host using tools like Snort or Suricata.
- Case Study: Mitigation of a DDoS attack by implementing aggressive rate limiting and connection tracking rules in the host firewall.

Module 6: Auditing, Logging, and Threat Detection

- Configuring Auditd for comprehensive system auditing and tracking critical events.
- Centralized log management using rsyslog or syslog-ng integration.
- Integrating Linux logs with SIEM solutions for analysis.
- Detecting Indicators of Compromise and suspicious process activity.
- Performing log rotation and ensuring secure, non-repudiable log storage for compliance.
- Case Study: Identifying a successful lateral movement attempt by correlating suspicious authentication logs with unusual process execution records in a SIEM dashboard.

Module 7: Data Protection and Encryption

- Implementing disk encryption using LUKS for data at rest protection.
- Securing data transmission with OpenSSL and TLS/SSL certificate management.
- Configuration of secure backup and disaster recovery mechanisms
- File system level access control using ACLs
- Securing web services and applications running on Linux
- Case Study: Restoration of critical application data following a ransomware attack, emphasizing the importance of secure, segmented, and encrypted backups.

Module 8: Incident Response and Best Practices

- Formulating a Linux-specific Incident Response plan and procedures.
- Techniques for live system forensic acquisition and evidence preservation.
- Applying a continuous vulnerability management cycle
- Introduction to DevSecOps principles for embedding security early in the development lifecycle.
- Review of major security standards and frameworks relating to Linux security.
- Case Study: Simulating a security incident and performing a full response, triage, remediation, and post-mortem analysis in a dedicated lab environment.

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