Advanced Linux for Cyber Analysts Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Advanced Linux skills are essential for cyber analysts tasked with securing enterprise environments, detecting threats, and responding to incidents in real time. Linux serves as the backbone of modern IT infrastructures, cloud environments, and security operations, making mastery of its command-line tools, scripting capabilities, system monitoring, and security utilities critical for effective cyber defense. Advanced Linux for Cyber Analysts Training Course provides a hands-on, in-depth exploration of advanced Linux techniques used in cybersecurity, including kernel and process management, network monitoring, forensic analysis, threat detection, and automation through scripting and open-source tools.

Participants will gain practical experience in configuring, hardening, and monitoring Linux environments to detect, analyze, and respond to cyber threats. The course emphasizes real-world scenarios and case studies, enabling learners to integrate Linux knowledge with cyber threat intelligence, vulnerability management, intrusion detection systems, and incident response workflows. By the end of this course, cyber analysts will be equipped to apply Linux tools and strategies effectively, enhancing organizational security posture and operational resilience.

Programme Curriculum

Advanced Linux for Cyber Analysts Training Course

Introduction

Advanced Linux skills are essential for cyber analysts tasked with securing enterprise environments, detecting threats, and responding to incidents in real time. Linux serves as the backbone of modern IT infrastructures, cloud environments, and security operations, making mastery of its command-line tools, scripting capabilities, system monitoring, and security utilities critical for effective cyber defense. Advanced Linux for Cyber Analysts Training Course provides a hands-on, in-depth exploration of advanced Linux techniques used in cybersecurity,

including kernel and process management, network monitoring, forensic analysis, threat detection, and automation through scripting and open-source tools.

Participants will gain practical experience in configuring, hardening, and monitoring Linux environments to detect, analyze, and respond to cyber threats. The course emphasizes real-world scenarios and case studies, enabling learners to integrate Linux knowledge with cyber threat intelligence, vulnerability management, intrusion detection systems, and incident response workflows. By the end of this course, cyber analysts will be equipped to apply Linux tools and strategies effectively, enhancing organizational security posture and operational resilience.

Course Objectives

1. Master advanced Linux commands, shell scripting, and automation for cyber analysis.
2. Configure and harden Linux systems to prevent unauthorized access.
3. Monitor system logs and processes for suspicious activities.
4. Conduct network analysis and packet inspection using Linux-based tools.
5. Implement intrusion detection and prevention techniques on Linux servers.
6. Perform forensic investigations using Linux utilities and open-source frameworks.
7. Analyze malware behavior and system compromise in Linux environments.
8. Apply threat hunting methodologies leveraging Linux tools and scripts.
9. Integrate Linux systems with Security Information and Event Management (SIEM) platforms.
10. Conduct vulnerability assessments and patch management using Linux.
11. Automate repetitive cyber defense tasks via scripting and cron jobs.
12. Develop Linux-based reporting and visualization of security metrics.
13. Ensure compliance with cybersecurity frameworks and standards in Linux environments.

Organizational Benefits

- Strengthened cybersecurity posture through advanced Linux monitoring
- Improved threat detection and incident response capabilities
- Enhanced forensic investigation and root cause analysis
- Reduced system vulnerabilities and misconfigurations
- Greater operational efficiency through automation and scripting
- Better integration with SIEM, IDS, and SOC workflows
- Reduced risk of data breaches and unauthorized access
- Enhanced reporting, auditing, and compliance processes
- Empowered IT and security teams with advanced Linux skills
- Increased resilience of critical systems and infrastructure

Target Audiences

- Cybersecurity analysts and incident responders
- Linux system administrators
- Threat hunters and SOC operators
- Security engineers and architects
- IT auditors and compliance officers
- Penetration testers and ethical hackers
- Forensic analysts and malware researchers
- IT managers overseeing security operations

Course Duration: 10 days

Course Modules

Module 1: Advanced Linux Command-Line Skills

- Master shell navigation, text processing, and file manipulation commands
- Use advanced pipelines, filters, and regular expressions
- Automate tasks using Bash scripting
- Manage system processes and job scheduling
- Configure environment variables for security operations
- Case Study: Automating log analysis with shell scripts

Module 2: Linux System Hardening

- Apply best practices for securing Linux servers
- Configure user permissions, sudoers, and authentication mechanisms
- Implement file system security and access controls
- Harden network services and ports
- Enable and configure firewall and SELinux/AppArmor policies
- Case Study: Hardening a production Linux server against attacks

Module 3: Process & Kernel Monitoring

- Monitor running processes, threads, and services
- Analyze kernel messages and system logs for anomalies
- Use monitoring tools such as top, htop, ps, and dstat
- Understand Linux kernel modules and drivers for security
- Detect malicious processes and hidden rootkits
- Case Study: Detecting unauthorized processes on a critical server

Module 4: Network Analysis & Packet Inspection

- Capture and analyze network packets using tcpdump and Wireshark
- Inspect TCP/IP stack and network interfaces
- Monitor traffic for unusual patterns and anomalies
- Use netstat, ss, and ip commands for network troubleshooting
- Identify unauthorized connections and suspicious traffic
- Case Study: Investigating a network breach using Linux tools

Module 5: Log Management & Security Monitoring

- Collect, centralize, and analyze system logs
- Configure syslog, rsyslog, and journald for monitoring
- Detect anomalies in authentication and system events
- Use log analysis tools for incident response
- Integrate logs with SIEM platforms for real-time alerting
- Case Study: Investigating failed login attempts and privilege escalation

Module 6: Intrusion Detection & Prevention

- Deploy and configure host-based intrusion detection systems (HIDS)
- Monitor file integrity and system behavior for malicious activity
- Configure Snort or Suricata for intrusion detection

- Analyze alerts and prioritize incidents
- Implement automated responses to detected threats
- Case Study: Responding to a simulated intrusion using Linux IDS

Module 7: Forensic Investigation Techniques

- Collect evidence without altering system state
- Examine file systems, memory dumps, and logs
- Recover deleted files and investigate suspicious artifacts
- Use Linux forensic tools such as SleuthKit and Autopsy
- Prepare forensic reports for internal or legal purposes
- Case Study: Forensic analysis of a compromised Linux workstation

Module 8: Malware Analysis on Linux

- Identify and isolate malware samples in Linux environments
- Analyze behavior using process monitoring and network analysis
- Reverse engineer scripts and binaries for threat intelligence
- Detect persistence mechanisms and rootkits
- Document and report malware findings
- Case Study: Analyzing a Linux ransomware attack

Module 9: Threat Hunting & Intelligence Gathering

- Use Linux tools for proactive threat hunting
- Monitor system indicators of compromise (IoCs)
- Collect threat intelligence from open-source platforms
- Automate threat detection using scripts
- Correlate system and network events for actionable insights
- Case Study: Hunting for stealthy attackers on Linux servers

Module 10: Vulnerability Assessment & Patch Management

- Scan Linux systems for vulnerabilities using open-source tools
- Analyze patch management processes and compliance gaps
- Remediate vulnerabilities without disrupting services
- Track and document vulnerability fixes
- Integrate findings into security risk dashboards
- Case Study: Conducting a vulnerability assessment for a Linux server farm

Module 11: Automation & Scripting for Cybersecurity

- Write Bash and Python scripts for routine security tasks
- Automate system monitoring, log parsing, and report generation
- Schedule automated tasks using cron jobs
- Use scripts for rapid incident response
- Maintain scripts securely and test for accuracy
- Case Study: Automating alert triage and reporting for SOC operations

Module 12: Security Tool Integration

- Integrate Linux with SIEM, IDS, and vulnerability scanners

- Configure logging and monitoring agents
- Collect and normalize data from Linux endpoints
- Build dashboards for security metrics
- Validate tool performance and alert accuracy
- Case Study: Integrating Linux logs with a SIEM platform

Module 13: Compliance & Governance

- Implement security policies aligned with cybersecurity frameworks
- Document configurations, monitoring, and incident response plans
- Conduct internal audits and policy compliance checks
- Track regulatory requirements for Linux-based infrastructure
- Report compliance status to management and regulators
- Case Study: Ensuring compliance with ISO/IEC 27001 on Linux servers

Module 14: Incident Response & Recovery

- Prepare incident response plans specific to Linux environments
- Investigate, contain, and remediate security incidents
- Recover compromised systems and validate integrity
- Conduct root cause analysis and lessons learned
- Update policies and playbooks based on incidents
- Case Study: Responding to a simulated Linux ransomware outbreak

Module 15: Advanced Security Analytics & Reporting

- Use Linux-based analytics tools for security intelligence
- Generate actionable security metrics and reports
- Correlate events across multiple endpoints
- Visualize security trends for SOC and management dashboards
- Recommend improvements based on analytics insights
- Case Study: Reporting and mitigating persistent threats in enterprise Linux

Training Methodology

- Instructor-led presentations and live demonstrations
- Hands-on labs and practical exercises on Linux environments
- Real-world case study analysis and scenario simulations
- Group exercises, problem-solving tasks, and collaborative labs
- Use of open-source Linux security and monitoring tools
- Continuous assessments, quizzes, and feedback sessions

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	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 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