BLACKBIRD FOR TRAINING

Advanced Linux for Security & Forensics

4 – 8 April 2027
Cairo (Egypt)

UK Traininig
PARTNER



www.blackbird-training.com

Advanced Linux for Security & Forensics

Ref: 3255097_331730 **Date:** 4 – 8 April 2027 **Location:** Cairo (Egypt) **Fees:** 4900 GBP

Introduction

Advanced Linux is a critical skill set for professionals managing complex IT environments, optimizing system performance, and implementing advanced security and forensic techniques. This course equips participants with the technical depth and practical skills to handle enterprise-grade Linux systems, automate processes, troubleshoot complex issues, and conduct security investigations.
Designed for professionals seeking mastery beyond the basics, the program focuses on real-world scenarios, advanced configurations, system hardening, performance tuning, and in-depth investigation techniques to secure and optimize critical infrastructure.

Course Objectives

- Master advanced Linux command-line tools and shell scripting.
- Configure and optimize system performance for production environments.
- Manage advanced networking, routing, and firewall configurations.
- Implement security best practices and system hardening techniques.
- Conduct forensic investigations and incident analysis on Linux systems.
- Automate administrative tasks using scripting and configuration management tools.
- Diagnose and resolve complex system issues effectively.
- Integrate monitoring, logging, and auditing for compliance.

Course Outlines

Day 1: Advanced Linux System Administration

- Deep dive into advanced file system management.
- Managing kernel modules and parameters.
- Advanced user and group administration.
- Process management and job scheduling.
- Advanced package management techniques.
- Workshop: Customizing Linux system behavior.



Day 2: Networking & Firewall Configuration

- Configuring advanced network interfaces and routing.
- Using iptables/nftables for custom firewall rules.
- Network performance optimization.
- Troubleshooting connectivity issues.
- Secure remote management and tunneling.
- Lab: Designing secure network configurations.

Day 3: Investigation & Forensics

- Fundamentals of Linux forensics.
- Preserving and collecting digital evidence.
- File system and log analysis techniques.
- Detecting and investigating system breaches.
- Tools for forensic imaging and recovery.
- Practical exercise: Analyzing a compromised system.

Day 4: Security & System Hardening

- Implementing advanced security policies.
- Enforcing access controls and privilege management.
- Auditing system activities and monitoring logs.
- Applying patches and managing vulnerabilities.
- Intrusion detection and prevention methods.
- Case study: Securing a production Linux server.

Day 5: Automation & Performance Optimization

- Writing advanced shell scripts for automation.
- Integrating configuration management tools Ansible, Puppet, etc..
- Performance tuning for CPU, memory, and I/O.
- Monitoring system health and resource usage.
- Final project: Designing a secure, optimized, automated Linux environment.
- Course closure and certification.



Why Attend this Course: Wins & Losses!

- Develop deep expertise in advanced Linux administration.
- Gain hands-on experience with investigation and forensic techniques.
- Improve system security, reliability, and performance.
- Automate repetitive tasks to increase efficiency.
- Learn to respond effectively to security incidents.
- Apply knowledge directly to enterprise-scale environments.
- Strengthen decision-making through data-driven system analysis.
- Earn a professional certification to boost career prospects.

Conclusion

The Advanced Linux course delivers a complete toolkit for mastering system administration, security, and forensic investigation in enterprise environments. By combining theoretical concepts with extensive practical exercises, it prepares participants to configure, secure, and troubleshoot Linux systems at the highest professional level.

Graduates of this program will be equipped to design secure infrastructures, automate complex workflows, and perform in-depth investigations — ensuring operational resilience and compliance in any organization.

