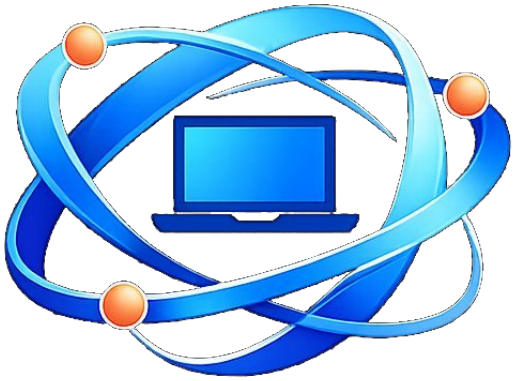

MFE-IT

Reference: 2B/EN/LS

Linux Security Training Course

Auditing, Hardening and Protecting Production Systems

Duration: 4 Days | Hours: 28 h

Remote · Sessions guaranteed from 1 registrant · 60% hands-on practice

DESCRIPTION

Linux systems are powerful, but their security depends entirely on their configuration. A default install — even on a hardened distribution — leaves many doors open: unnecessary services, weak SSH defaults, lax permissions and insufficient logging. Hardening is not optional in production: it is the baseline.

This Linux Security training course guides you step by step through the implementation of best practices for securing a Linux server: system hardening, access management, control of exposed services and protection against intrusions. The approach is production-oriented, with checklists and open-source tools that you can apply immediately on Debian, Ubuntu, RHEL or any modern distribution.

LEARNING OBJECTIVES

By the end of this training course, participants will be able to:

- Identify common vulnerabilities in Linux systems
- Implement a structured system hardening plan
- Secure SSH access, users and critical services
- Implement effective logging and monitoring of abnormal behaviour
- Configure a local firewall (iptables, ufw, nftables) and limit the attack surface
- Perform automated security audits with open-source tools

PREREQUISITES

- Solid foundation in Linux administration (users, services, files, shell)
- Comfortable with command lines and server environments
- Basic network knowledge desirable

> *Because each participant is unique, a personalised interview is systematically organised in advance with our expert to design a training programme perfectly aligned with their objectives, level and professional challenges.*

TARGET AUDIENCE

System administrators, IT technicians, security consultants and DevSecOps teams seeking to strengthen the security of their Linux infrastructures locally, in the cloud or in hybrid environments.

DETAILED PROGRAMME

> The training alternates between theoretical input and hands-on practice (approximately 60% of the time). Modules are built around practical exercises based on real-world business use cases.

Module 1 – Initial Assessment and Linux Security Principles

- Typical vulnerabilities in Linux deployments
- Good security practices and secure system architecture
- Preliminary testing and baseline assessment

Module 2 – System Hardening

- Removal of unnecessary services and packages
- Locking critical files and directories
- sysctl configuration and kernel-level restrictions

Module 3 – User Management and Authentication

- Password policies and PAM configuration
- sudo restrictions and login logs
- SSH key authentication and fail2ban automatic banning

Module 4 – Network Security and Firewalls

- Address and port filtering with iptables, ufw, nftables
- Secure SSH configuration and port hardening
- Closing unnecessary ports and network segmentation

Module 5 – Monitoring, Alerts and Logging

- System logs: journalctl, rsyslog and log rotation
- Integration with monitoring tools or SIEM
- Anomaly detection and alerting

Module 6 – Security Audit and Open-Source Tools

- Vulnerability analysis with Lynis, Tiger and OpenSCAP
- SELinux and AppArmor mandatory access control
- Automatic report generation and remediation recommendations

TEACHING METHODS

Format and Delivery

The training is delivered remotely via an interactive virtual classroom. It can also be delivered on-site, with content customised to match the needs of your professional project. The theory/practice split is approximately 40%/60%.

MFE-IT Ultra-Personalised Format

Each session accommodates between 1 and 3 participants, ensuring highly individualised support. A preliminary interview allows us to tailor the content to each participant's profile. Inter-company sessions are guaranteed from just 1 registrant (except in cases of force majeure).

Skills Assessment

Throughout the training, the trainer assesses participant progress through multiple-choice questions, role-playing exercises and hands-on work. At the end, a certificate of achievement is issued to each participant.

Post-Training Support

For one month following the training, each participant can contact MFE-IT trainers with questions about implementing acquired knowledge. A response is provided by email or telephone within 48 working hours.

Accessibility

MFE-IT is committed to welcoming people with disabilities. Contact: contact@mfe-it.com.

PRACTICAL INFORMATION

Trainer Resources

- Structured demonstrations aligned with the detailed programme
- Exercise briefs and solutions throughout the training
- A ready-to-use technical environment for practical workshops
- Trainer validation of acquired knowledge at the end of each workshop
- Digital reference documents

Certification and Validation

At the end of the training, a certificate is sent by email specifying the objectives, nature, duration and assessment results. A completion certificate can also be provided on request.

Benefits for Participants

- Train from your workplace or home, with no travel required
- Benefit from an expert trainer-consultant on the subject
- Enjoy an ultra-personalised format (1 to 3 participants)
- Continue training even in the event of unforeseen circumstances

Benefits for the Organisation

- Optimise the training budget by reducing travel and accommodation costs
- Offer quality training to all employees, regardless of location
- Reduce absence time linked to travel
- Support team upskilling in all contexts