

GWENDAL LE COGUIC

COURSES

Each training session focuses on practical demonstrations, interactive exercises, and discussions based on real-life situations to ensure the acquisition of key skills.

Each session can be taken:

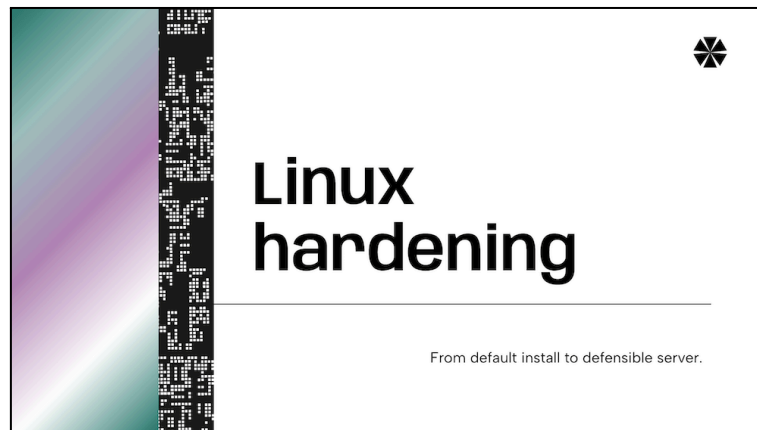
- on-site or remotely
- in French or English
- individually or in groups

Quotes available upon request

Tel: +33 7 69 02 25 10

Email: contact@glc.st

LINUX HARDENING



a. Description

This intensive 1-day training teaches you how to harden a Linux server from the ground up. You'll learn to **minimize the system footprint, lock down user privileges, secure network exposure, and reinforce critical services**. Through hands-on exercises, you'll apply **real-world hardening** techniques used by security professionals.

b. Educational goals

- Identify common entry points, privilege-escalation paths, and misconfigurations
- Minimize installed software and apply kernel and filesystem protections
- Configure strong authentication, secure sudo policies, and controlled user environments
- Secure network interfaces, firewall rules, and remote access pathways
- Deploy logging, auditing, and basic intrusion-detection mechanisms

c. Prerequisites

- Being comfortable with CLI mode
- Familiarity with basic Linux administration

d. Targeted audience

- System administrators
- Dev(Sec)Ops engineers

e. Program

Introduction

- Why hardening matters?
- Understanding the attack surface
- Defense in depth
- Principle of least privilege
- Minimal install philosophy
- Hardening is role-specific
- Reference frameworks
- Baseline vs. hardening vs. compliance

System baseline

- Partitioning strategy
- Unnecessary packages & services
- Unused kernel modules
- Hardening the Kernel

Account hardening

- Mandatory Access Control (MAC)
- Account and sudo hardening
- Password and authentication policy

Network hardening

- Network exposure
- Firewalling
- Brute-force mitigation

Services hardening

- Dedicated users
- File permissions
- Service sandboxing

Filesystem, permissions & integrity

- SUID/SGID auditing
- Sticky bit and ACLs
- Immutable attributes
- File integrity monitoring

Logging, auditing & monitoring

- Kernel-level security event
- Centralized logging
- Intrusion detection concepts

Automation & compliance validation

- Scoring with Lynis
- Formal compliance scoring with OpenSCAP
- Hardening-as-code with Ansible

Resources

- Books
- Interactive platforms
- Courses & videos
- Tools