

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

INTRODUCTION TO PENTESTING



a. Description

*The Pentest training is an intensive 3-day program designed to introduce **developers, system administrators** and any **cybersecurity enthusiasts** to the fundamentals of **ethical hacking**. Through a combination of **theory** and **practical exercises** in dedicated environments, participants will learn how to **identify and exploit vulnerabilities** in web applications and network services. Essential tools such as **Kali Linux, Metasploit, Burp Suite** and more will be covered. At the end of the training, participants will be able to conduct effective security audits and strengthen the protection of their IT infrastructures.*

b. Educational goals

- Understand the fundamentals of ethical hacking and legal boundaries
- Identify and analyze common vulnerabilities in web and network systems
- Use industry-standard tools like *Kali Linux, Metasploit, and Burp Suite*
- Perform manual exploitation techniques
- Conduct vulnerability assessments and interpret scan results
- Apply pentesting methodologies to simulate real-world attacks

c. Prerequisites

- Basic knowledge of IT systems and networks
- Familiarity with operating systems (Linux and Windows)
- Basic understanding of programming or scripting is a plus but not required

d. Targeted audience

- Developers
- System administrators
- Dev(Sec)Ops engineers
- Any cybersecurity enthusiasts

e. Program

Day 1 - Introduction and information gathering

Audit charter

- What is it?
- Content of the audit charter

Methodology

- Steps of an attack
- An attacker's bag of tricks
- Testing process

Introduction to Kali Linux

- What is it?
- Tools included
- Lab configuration

Information gathering

- Passive vs. active recon
- *Google, Shodan, GitHub* hacking
- Collect Companies and employees data
- Technologies
- ASN enumeration
- DNS enumeration, resolution and probing
- Port scan

Vulnerability scan

- CWEs, CVEs & CVSS
- Scanners

Day 2 - Exploitation techniques and web security

Report

- What is it?
- Content of the report

HTTP testing

- Requirements
- What would you test?
- Browser extensions
- Introduction to *Burp Suite*
- Cross-Site Scripting
- SQL injection
- Arbitrary file upload

Other network services

- Shell vs. reverse shell
- Find, install and use exploits
- Introduction to *Metasploit*
- Service exploitation: *FTP, SMB, PostgreSQL, WebDAV...*

Day 3 - Post-exploitation and password attacks

Final presentation

- What is it?

Password attacks

- Cryptography refresher: encoding, hashing, encryption
- Leaked passwords and default passwords
- Online services & network attacks
- Wordlists
- Linux vs. Windows

Privilege escalation

- Horizontal vs. Vertical
- Linux vs. Windows

Post-exploitation

- Persistency
- Antivirus evasion
- Port forwarding and port tunneling