Updated on 22/08/2025

Sign up

Pentesting training - Performing penetration tests

5 days (35 hours)

Presentation

Today, penetration tests (or pentests) are the reference tool for validating the robustness of an information system in the face of increasingly sophisticated cyber threats. This "Pentesting: Performing penetration tests" training course will give you the skills you need to identify, exploit and correct vulnerabilities while complying with the French (Godfrain law, LCEN) and European (NIS 2, RGPD) legal frameworks.

During this training course, you will discover the fundamentals of pentesting and its positioning in risk management, while integrating the legal, ethical and organizational dimensions specific to the discipline. You will learn how to plan a mission, define a scope of intervention and gather the necessary information using OSINT and reconnaissance techniques.

You will be guided in the use of state-of-the-art tools and methods for scanning, vulnerability analysis, web application, network and system exploitation, as well as for post-exploitation, lateral movement and data exfiltration. Client-side attacks and social engineering will also be covered to complete your understanding of modern compromise vectors.

A strong emphasis will be placed on methodology and reporting: drafting clear audit reports, building proof-of-exploitation (POC) and formulating concrete recommendations for technical and managerial teams.

As with all our sessions, this program is based on the latest stable version of the tools and incorporates the critical CVEs of 2025, to ensure that you are always up to date.

Objectives

- Understand the fundamentals and legal framework of pentesting

- Understand the different phases of penetration testing
- Use pentesting analysis tools and techniques
- Simulate attacks
- Write a professional audit report

Target audience

- CISOS
- Technicians
- Auditors involved in pentesting
- System and network administrators

Prerequisites

- Basic knowledge of IT and information systems security

Pentesting Training Program

[Day 1 - Morning]

Overview of pentesting and threats

- Definition of penetration testing; black-, grey-, white-box
- Actors & motivations: cyber-crime, hacktivism, espionage
- Positioning pentesting in risk management (ISO 27005)
- Understanding the fundamentals of pentesting
- Practical workshop: Mapping the attack surface of a fictitious IS.

[Day 1 - Afternoon]

Legal framework, compliance and ethics

- Applicable French (LCEN, Godfrain law) & EU (NIS 2, RGPD) legislation
- Criminal/civil liability; confidentiality agreements (NDA)
- Standards & benchmarks: PTES, OSSTMM, ISO/IEC 17025
- Understanding the legal framework for compliant and controlled testing
- Practical workshop: Analyze an engagement letter and identify critical clauses.

Scoping and planning the mission

- Gathering customer requirements, scope & objectives
- Risk analysis: technical constraints, planning, resources

- Choice of approaches: black-box vs grey-box vs white-box
- Practical workshop: Drawing up a test plan and a simplified RACI.

[Day 2 - Morning]

OSINT and passive recognition

- WHOIS, Shodan, DNS archives, social networks
- Metadata extraction & Google dorks
- Initial asset mapping / target prioritization
- Practical workshop: Extracting info on a public target via SpiderFoot.

[Day 2 - Afternoon]

Active scan & network enumeration

- Network discovery: Nmap, Masscan, fingerprinting
- Banner grabbing & version detection
- Identification of wireless / IoT devices
- Practical workshop: Perform a full Nmap scan and interpret the results.

Vulnerability scanning

- Automatic scanners (Nessus, OpenVAS) vs. manual analysis
- CVSS scoring; correlation with business criticality
- False positive / false negative management
- Practical workshop: Qualifying critical vulnerabilities in an OpenVAS report.

[Day 3 - Morning]

Web application exploitation

- OWASP Top 10: SQLi, XSS, SSRF, etc.
- Tools: Burp Suite Pro, SQLmap; WAF bypass
- Escalation of logical privileges (IDOR, business logic)
- Practical workshop: Exploiting an XSS vulnerability stored in Juice Shop.

[Day 3 - Afternoon] Network &

system exploitation

- Remote exploits (SMB, RDP) & Metasploit
- Modern buffer overflow (ROP, ASLR bypass)
- Password cracking, pass-the-hash, Kerberoasting
- Simulate realistic attacks to test the resilience of an information system.
- Practical workshop: Compromising a Windows server via EternalBlue.

Social engineering & client-side attacks

- Phishing / spear-phishing: kits, success metrics
- Macro attacks, HTA, USB Rubber Ducky
- Basic EDR bypasses
- Practical workshop: Launching a phishing campaign in a GoPhish lab.

[Day 4 - Morning]

Post-exploitation and privilege escalation

- Advanced local enumeration (LinPEAS, WinPEAS)
- Exploitation of weak services, scheduled tasks, local CVEs
- Credential plundering (LSASS, SAM, Mimikatz)
- Practical workshop: Obtaining SYSTEM on a vulnerable VM.

[Day 4 - Afternoon]

Lateral movement & persistence

- Pass-the-Ticket, WMI, PsExec, SSH trust
- Backdoors: scheduled tasks, registry, cron
- Evasion techniques & OPSEC during intrusion
- Practical workshop: Pivoting to a subnet via proxychains.

Exfiltration & cleaning

- Exfiltration: DNS tunnelling, HTTPS covert channel
- Data compression, encryption, steganography
- Anti-forensic: deleting logs & artifacts
- Practical workshop: Exfiltrating documents via an encrypted DNS channel.

[Day 5 - Morning]

End-to-end attack simulation

- C2 implementation (Cobalt Strike / Sliver)
- Complete chain: recon, exploit, C2, exfiltration
- Collection of IOCs & generation of logs for blue-team
- Practical workshop: timed CTF "Capture The Flag" challenge.

[Day 5 - Afternoon] Audit report

preparation

- Structure: executive summary, findings, POC, remedies
- Metrics: CVSS, kill-chain, MITRE ATT&CK mapping
- Prioritized action plan & quick wins
- Write a clear, professional audit report that can be used by technical teams and decision-makers.
- Practical workshop: Writing a peer-reviewed critical vulnerability report.

Debriefing & continuous improvement

- Oral presentation of results; management of sensitive issues
- Maturity frameworks: OSCP, NIST, purple-teaming
- Capitalization: reusable scripts & vulnerability watch
- Practical workshop: team retrospective & continuous improvement plan.

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire enabling us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples and

and group work sessions.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Certification

A certificate will be awarded to each trainee who has completed the entire course.