+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated 05/08/2025

Sign up

# Pentesting training - Performing penetration tests

5 days (35 hours)

## Presentation

Master end-to-end penetration testing with this comprehensive pentesting training course, designed for IT professionals, DevSecOps and cybersecurity experts. You'll learn how to plan, execute and document effective tests on a variety of infrastructures, in compliance with legal frameworks and best practices.

You'll start with passive and active reconnaissance, using OSINT tools and techniques, network mapping, service enumeration and vulnerability scans.

You'll then learn how to exploit vulnerabilities on the web, network and system layers, use Metasploit, elevate your privileges and maintain post-exploitation access in Windows and Linux environments.

The course will take you through advanced attacks: Active Directory, Docker/K8s containers, evasion techniques, and multi-vector scenarios in simulated environments.

As with all our training courses, this one will be presented with the latest Pentesting updates.

## Objectives

- Understand the objectives, types, legal frameworks and methodologies of penetration testing
- Identify, map and analyze targets using passive and active reconnaissance techniques
- Exploit web, network, system and Active Directory vulnerabilities using dedicated tools
- Elevate privileges, maintain access and bypass detection and security mechanisms
- Write a structured pentest report with risk assessment and remediation recommendations
- Validate skills by carrying out a complete penetration test on a simulated simulated environment

## Target audience

- DevSecOps
- Pentester

## Prerequisites

- knowledge of Linux and Windows systems
- basic network skills

## JUnit : Efficient Java testing

### Introduction to pentesting

- Definition, objectives, scope (web, infra, mobile, IoT...)
- Differences between Pentest, Red Team, Vulnerability Audit
- Types of testing (black box, gray box, white box)
- Legal and ethical framework

### Preparing a penetration test

- Understanding the customer's objectives and scope
- Writing an engagement letter
- Choice of tools and methodology

### Passive reconnaissance

- OSINT
- DNS analysis
- Leak detection

### Active reconnaissance

- Port scan
- Service and banner detection
- OS fingerprinting
- Vulnerability scanning

## Advanced enumeration

- SMB, LDAP, FTP, SNMP enumeration
- NetBIOS / Kerberos scanning
- Web enumeration
- Internal network enumeration

## Pentest Web - Introduction

- OWASP Top 10: panorama of major vulnerabilities
- Fuzzing with wfuzz, ffuf, Dirb
- Technology detection

## Classic Web attacks

- SQL injection
- Command Injection / RCE
- File Inclusion
- Cross-Site Scripting
- Cross-Site Request Forgery

## Web attack automation

- Burp Suite
- ZAP Proxy
- Nikto / wapiti / OWASP ZAP CLI

## Network and services exploitation

- SMB vulnerabilities

- FTP, RDP, Telnet vulnerabilities
- DNS exploitation
- Man-in-the-Middle

## System takeover

- Public exploits
- Metasploit Framework
- Reverse shell and bind shell
- Post-exploitation with Metasploit

## Privilege escalation

- System enumeration
- SUID, Scheduled Tasks, Unquoted Service Path privileges
- Exploiting local vulnerabilities
- Credential plundering

## Persistence and cleaning

- Persistence techniques
- Rootkits and persistent shells
- Erasing traces

## Attacking an Active Directory environment

- AD enumeration
- Kerberoasting / AS-REP roasting
- Pass-the-Hash / Pass-the-Ticket / Golden Ticket
- Exploiting GPOs, ACLs and delegations

## Container security

- Introduction to Docker and Kubernetes
- Common vulnerabilities

- Container-to-host breakout
- Tools: Dockerscan, kube-hunter

### Evasion techniques

- Antivirus Evasion
- Bypass EDR: LOLBAS, living-off-the-land
- Custom payloads with msfvenom / Veil / Unicorn

### Perform a multi-vector test

- Combined attack scenario: web ? RCE ? reverse shell ? AD
- Red Team approach on a simulated lab

## Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer 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 which enables 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, with brainstorming sessions and group work.

## Validation

At the end of the session, a multiple-choice questionnaire is used to verify the correct acquisition

skills.

## Certification

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