CompTIA Penetration Testing (PENTEST+)

Description

Master penetration testing with the CompTIA Penetration Testing (PENTEST+) certification

The CompTIA Penetration Testing (PENTEST+) training is ideal for cybersecurity professionals looking to deepen their skills in penetration testing. In this intensive program, you will learn how to plan, execute, and analyze comprehensive tests to identify system vulnerabilities. Whether you are a pentester, analyst, or operator, this certification will help you demonstrate your expertise in a rapidly evolving field. With the rise of cyber threats, this training offers valuable skills to secure companies' networks and applications.

In addition to comprehensive preparation for the PT0-002 exam, you will acquire practical skills through virtual labs and real-world exercises. You will learn to use tools and scripts to collect, analyze, and exploit data in various network environments. This training allows you to become an indispensable asset to any security team, mastering the entire penetration testing process from planning to comprehensive report writing.

Course Content
Module 1: Planning and defining the scope of penetration tests

- Overview of penetration testing methods
- Planning a PenTest operation
- Assessing and negotiating a PenTest service
- Preparation for conducting penetration tests

Module 2: Conducting passive reconnaissance

- Collecting general data
- Preparing base data for upcoming actions

Module 3: Performing penetration tests

- Conducting social engineering tests
- Performing physical security tests on infrastructures

Module 4: Conducting active reconnaissance

- Scanning networks
- Identifying data sources
- Detecting vulnerability risks
- Basic script analysis

Module 5: Analyzing vulnerability factors

- Analysis of vulnerability detection results
- Extracting data for network test preparation

Module 6: Penetrating communication networks

- Exploiting vulnerabilities in wired, wireless, and radio frequency systems
- Exploiting vulnerabilities in specific networks

Module 7: Analyzing host-based vulnerabilities

- Analysis of Windows operating system vulnerabilities
- Analysis of Linux operating system vulnerabilities

Module 8: Testing software and applications

- Exploiting vulnerabilities in Web apps
- Testing software and application source code (including compilation)

Module 9: Completing post-exploitation activities

- Using lateral movement techniques
- Employing persistence techniques
- Applying anti-forensic techniques

Module 10: Writing a penetration test report

- Analyzing penetration test results
- Developing mitigation strategy recommendations
- Writing and managing a report
- Completing post-report tasks

Documentation

- Digital course materials included

Exam

- This course prepares to the CompTIA PenTest+ certification
- In order to receive the CompTIA PenTest+ certification, learners must pass two exams: PT0-002.
- If you wish to take these exams, please contact our secretariat who will let you know the cost of the exam and will take care of all the necessary administrative procedures for you.

Participant profiles

- Pentesters
- Cybersecurity analysts
- Vulnerability testers

- Information systems security managers
- Security consultants

Prerequisites

- Mastery of network and security concepts
- Experience with penetration testing tools like Metasploit
- Knowledge of operating systems (Windows, Linux)
- Ability to use Bash, Python, Ruby, or PowerShell scripts
- Understanding of network protocols (TCP/IP, DNS, HTTP)

Objectives

- Plan and organize penetration tests
- Exploit vulnerabilities in wired and wireless networks
- Collect and analyze data to detect weaknesses
- Use scripts to automate tests
- Analyze system and application vulnerabilities
- Develop and write penetration test reports

Description
CompTIA Penetration Testing (PENTEST+) training
Niveau
Intermédiaire
Classroom Registration Price (CHF)
4000
Virtual Classroom Registration Price (CHF)
3750
Duration (in Days)
5
Reference
COM-202