Updated 03/25/2025

Sign up

CompTIA Pentest+ Certification Training (PT0-002)

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

5 days (35 hours)

Presentation

Our Comptia Pentest+© training course will prepare you effectively for certification. This certification will enable you to prove your skills in penetration testing and IT security, reinforcing your credibility and value on the professional market.

Our training covers all the skills needed to identify, exploit and document vulnerabilities in systems, networks and applications.

This course provides you with the expertise you need to pass the PT0-002 exam, developing skills that can be applied directly in the workplace.

We are constantly updating our program to reflect the latest developments the industry and ensure that our learners have the most up-to-date skills.

Training content

- 4-day training with a certified expert
- 1 year self-study access to the Labs
- 1 pass for certification

Objectives

- Understand the fundamentals of penetration and associated regulatory frameworks (RGPD, PCI DSS)

- Know how to plan, execute and document an intrusion , from collection to remediation
- Exploit network, application and system vulnerabilities using professional tools (Nmap, Nessus, Metasploit, etc.).
- Master the art of writing clear, usable reports for different audiences (technical and non-technical).
- Develop communication and report writing skills

Target audience

- Pentesters
- Cybersecurity Analysts
- Security Consultants
- System administrators

Prerequisites

- 3 to 4 yearspractical experience in performing penetration tests, vulnerability and code analysis
- Solid knowledge of IT security
- Basic knowledge of penetration testing
- Knowledge of scripting languages such as Python or Ruby

Software requirements

- Virtualization environment (VMware or VirtualBox)
- Vulnerability testing tools (Nmap, Metasploit, Burp Suite, OWASP ZAP, SQLmap...)
- Tools for password management and secure storage of sensitive information

Note: Ambient IT is not the owner of Comptia Certifications©, this certification belongs to Comptia®, Inc.

Pentest+© Certification Preparation Program

Introduction to PenTest+ certification

- PenTest certification objectives
- Fundamentals of penetration testing
- Presentation of the tools and environments required

Planning and Scoping

- Understanding regulatory frameworks (RGPD, PCI DSS)
- Rules of engagement and legal constraints
- Define test perimeters and targets
- Development of an appropriate strategy (testing in known and unknown environments)

Information gathering and vulnerability analysis

- **OSINT techniques (public information search)**
- Target analysis: network, applications, cloud
- **Use and prioritization of vulnerabilities (CVE, CWE)**

Exploitation and attacks

- Network exploitation techniques (ARP spoofing, VLAN hopping)
- Attacks on web applications (SQL injection, XSS, API)
- Exploiting mobile and IoT vulnerabilities
- Post-operation: persistence and lateral movements

Reports and remedies

- Writing reports tailored to technical and non-technical audiences
- Recommendations for vulnerability remediation
- System hardening techniques and best practices (patch management, MFA)
- Drafting and presentation of a final report

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 with regard to the training to come, 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% Practical, 40% Theory. Training material distributed in to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, brainstorming sessions and group work.

Validation

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

Sanction

A certificate will be issued to each trainee who completes the course.