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

Updated 20/03/2025

Sign up

CPTS Certification Training

All-In-One: Preparation & Exam included in price

3 days (21 hours)

Presentation

Our CPTS Certification training course will enable you to validate your practical and technical skills in offensive security and become a pentester. Penetration testing is practice of identifying, exploiting and documenting vulnerabilities in order to secure your IT infrastructures.

Our training program will teach you all the steps and techniques involved in a Pentesting analysis, and will enable you to take the CPTS certification exam at the end of the 3 days.

At the end of this course, you'll be able to identify, exploit and document vulnerabilities, and propose solutions to strengthen and optimize security.

Objectives

- Understand the fundamental concepts of pentesting.
- Identify and list an organization's technical vulnerabilities.
- Master the practical exploitation of identified vulnerabilities.
- Conduct advanced tests on web applications and internal systems.
- Propose relevant recommendations for long-term infrastructure security.
- Prepare for and pass the official CPTS certification exam.

Target audience

- Pentesters
- Cybersecurity Analysts
- Security Consultants

- System administrators

Prerequisites

- Solid knowledge of IT security
- Basic knowledge of penetration testing
- Knowledge of scripting languages such as Python or Ruby

CPTS Certification Training Program

Targeted recognition and information gathering

- Network approach with Nmap
- DNS enumeration and subdomains
- Identify vulnerable versions and Fingerprint the system
- SMB & FTP

Identifying and exploiting vulnerabilities

- Introduction to public exploits, Metasploit Framework
- Vulnerability scanning :
  - buffer
  - overflow
  - basics
- Exploiting common Web vulnerabilities
- Reverse shells and bind shells
- Malicious file transfer techniques

Advanced Web Application Security Testing

- SQLi (SQL injection), XSS (scripting)
- LFI/RFI file inclusion and CSRF attacks
- Security testing with Burp Suite
- Advanced handling of HTTP requests
- **FFUF**

Post-exploitation & Privileges

- Escalating privileges with Linux
- Escalating privileges with Windows
- Techniques for maintaining access
- Extraction of passwords/hashes

- SSH tunneling, network pivoting

Advanced intrusions in Active Directory environments

- Active Directory fundamentals
- Active Directory enumeration with BloodHound
- Pass-the-Hash attack and Kerberos exploitation
  - Kerberoasting
  - Golden Ticket
- LDAP

Pentest report & methodology

- Exam preparation tips and revision
- Standard OWASP/PTES methodology
- Vulnerability classification (CVSS)
- Technical results presentation

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 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 course: 60% Practical, 40% Theory. Training material distributed in digital format 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 is used to check correct acquisition.

skills.

Sanction

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