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

Updated 04/11/2024

Sign up

Training for TCM Security PNPT© certification

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

2 days (14 hours)

Presentation

The TCM Security Practical Network Penetration Tester (PNPT©) training course will give you all the resources you need to test the vulnerability of your systems, applications or corporate data.

With the help of this course, you'll become an expert at penetration testing a computer system or network, so you can spot any flaws that need to be fixed.

Thanks to PNPT© certification, you'll be able to increase your skills and knowledge in cybersecurity, and master effective ways of securing your IT system.

This training course will help you to demonstrate all the infringements present on your systems, with the aim of ensuring security in your company and a reliable environment.

Objectives

- Penetration testing skills
- Understanding different attack methods
- Solving system faults
- Securing a computer system
- Be ready for PNPT© certification

Target audience

- Ethical hackers

- Sliders
- Auditors
- SSI technicians
- Project managers

Prerequisites

Good knowledge of networks, systems and security.

Note: Ambient IT is not the owner of PNPT©, this certification belongs to TCM Security, Inc. ©.

TCM Security PNPT© training program

Tool introduction

- Introducing TCM Security
- Introduction to ethical hacking
- Advantages and disadvantages

External penetration test

- Vulnerability analysis and exploitation
- Attack connection portals (website, VPN, O365)
- Collecting information
  - On breached credentials
  - On social media
- Bypassing multi-factor authentication
- Listing third parties for data leaks
- Listing of services, ports and websites
- User name and account enumeration

Internal penetration test

- Swivel attacks
- Man-in-the-middle attacks (SMB relays, LDAP relays, IPv6 relays)
- Password and pass-the-hash attacks
- Kerberoasting attacks
- Vulnerability analysis and service enumeration
- Chop cracking

Social engineering

- SMS attacks (smshing)

- High-profile targeted attacks
- Phishing by e-mail
- Telephone attacks (vishing)
- Targeted attacks (spearphishing)

Web application testing

- Automated and manual injection tests (XSS, SQL)
- Directory route test
- Other manual tests depending on language and site content
- Malicious file downloads and remote code execution
- Password attacks and authentication bypasses
- Session attacks
- Website mapping
- Vulnerability analysis and exploitation

Physical penetration tests

- Recognition and information gathering
- Sensor bypass
- Hook
- Imitation
- Badge cloning
- Piggy backing

Companies concerned

This training 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 inputs from the trainer supported by examples and

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.