Updated on 15/05/2024

Sign up

eLearnSecurity eCPPT© Certification Training

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

Presentation

Our eCPPT© certification preparation course will prove your pentesting skills through a 100% practical exam.

This cybersecurity exam contains the essential concepts for penetration testing: understanding the network, systems and web application attacks.

It consists of a practical test to assess your cyber-attack skills, as well as your ability to provide a comprehensive pentesting audit report.

Our training includes all the modules required for the exam, and the program can be adjusted to suit your needs. You'll review pentesting methods, vulnerabilities, exploits, scanning and exploit development.

You'll learn how to protect IT systems by understanding hacking methods. Finally, you'll learn the best practices for obtaining certification by taking a mock exam.

Training content

- 1 year self-study access to the Labs
- 4 expert coaching sessions: 4 days - 28 hours
- 1 certification pass

Objectives

- Strengthen your pentesting skills
- Be ready for eCPPT© certification

Target audience

- Safety managers
- Auditors
- Ethical hackers

Prerequisites

- Linux Shell experience
- Basic knowledge of Python
- Windows experience
- Use of Web proxy (Burp or equivalent)

Materials required

A virtual machine with Kali Linux installed.

Note: Ambient IT is not the owner of eCPPT©, this certification belongs to eLearnSecurity©.

eCPPT© Certification Preparation Program

Web application security

- Information gathering
- Cross Site Scripting
- SQL Injection
- Session Hijacking and Fixation
- Cross Site Request Forgery
- Vulnerabilities related to file and resource management

System security

- Fundamentals of architecture
- Debugger
- Buffer overflow
- Assembler development (Shellcoding)
- Cryptography and password cracking
- Malware

Network security

- Information gathering
- Scanning
- Listing
- Man in the middle (MitM)
- Operating
- After the operation

PowerShell for penetration testing

- Introduction
- Fundamentals
- Using PowerShell to attack

Linux operation

- Information gathering
- Remote operation
- After the operation

Wireless network security (Wi-Fi)

- Wireless network standards
- Discover a wifi network
- Traffic analysis
- Attacking a wireless network

eCPPT exam preparation

- Examination procedure
- Report writing
- Strategy for success

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 learning difficulties.

in-company security (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, with 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.