Updated 10/10/2024

Sign up

eLearnSecurity eCPPT© Certification Training

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

4 days (28 hours)

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.

Your understanding of hacking methods will help you protect your IT systems. Finally, you'll learn the best practices for obtaining certification through various training sessions.

Training content

- 6 months 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)
- Test My Knowledge

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

Information Gathering & Recognition

- Perform Host Discovery and Port Scanning on target networks
- List information from services running on open ports

Initial Access

- Enumerate User Names to identify Valid User Accounts on Target Systems
- Perform Password Spraying Attacks to Identify Valid Credentials for Initial Access
- Perform Brute Force Attacks on Remote Access Services for Initial Access

Web Application Penetration Testing

- Perform Web Application Enumeration to Identify Potential Vulnerabilities and Misconfigurations
- Identifying and Exploiting Common Vulnerabilities in Web Applications for Initial Access (SQLi, XSS, Command injection, etc.)
- Brute-force attacks on login forms
- Exploiting Vulnerable and Obsolete Web Application Components
- Exfiltrate Data and Identifiers from Compromised Web Applications and Databases

Operation & Post-Operation

- Identify and exploit vulnerabilities or misconfigurations in services
- Identifying and exploiting privilege escalation vulnerabilities
- Extracting and Breaking Password Hashes
- Identify Locally Stored Non-Secure Credentials

Exploit development

- Develop/Modify Exploit Code for Initial Access and Post-Exploitation
- Identify and exploit Memory Corruption vulnerabilities (Stack Overflow, Buffer Overflow)

Active Directory Penetration Test

- Active Directory Enumeration
- Identify Domain Accounts with Weak or Empty Passwords
- Perform AS-REP Roasting to Steal Kerberos Tickets for Authentication
- Perform Lateral Movement Techniques in Active Directory (Pass-the-Hash, Pass-the-Ticket)
- Get Domain Administrator Privileges/Access

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, 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.