

Updated on 11/03/2025

Register

OSCP™ Training (PEN-200)

ALL-IN-ONE: EXAM INCLUDED IN THE PRICE WITH THE PEN-200 COURSE

5 days (35 hours)

OVERVIEW

Keeping your infrastructure secure against cybercriminal attacks has become imperative. OSCP™ is OffSec's most renowned certification.

[Highly recognized in the market](#), this certification will prove your ethical hacking skills. You will learn how to perform pentests in a methodical and advanced manner.

This comprehensive OSCP™ training will allow you to improve your IT security knowledge and find the most complex security vulnerabilities.

All security vulnerabilities covered in the exam will be discussed, such as buffer overflows, web attacks, and Active Directory attacks.

You will learn how to master pentesting with Kali Linux, one of the most popular Linux distributions when it comes to intrusion testing.

After completing our bootcamp-style support program (half a day of training per week for two months), you will be eligible to take the certification exam.

Training content

- 90 days of access to self-study Labs
- 10 expert coaching sessions: 10 x Monday mornings (from 9 a.m. to 12:30 p.m.) per week (35 hours)
- 1 certification exam
- Access to the learner forum

OBJECTIVES

- Understand the main vulnerabilities and techniques used to hack into systems/websites
- Be able to break into a realistic network by putting your skills into practice in the lab
- Develop pentesting skills using the "Try harder" method
- Obtain OffSec Certified Professional (OSCP) certification

TARGET AUDIENCE

- Ethical hackers
- IT security experts
- Developers
- Technical architects
- Administrators
- Project managers
- People who have switched to IT security

Prerequisites

- Knowledge:
 - TCP/IP networks - Intermediate
 - Linux/Windows administration - Intermediate
 - Bash/Python scripting - Basic
- Proficiency in technical English
- Minimum personal investment of 2 hours per day to complete the labs
- [Refer to the technical requirements for participating in the proctored exam](#)
- [Test My Knowledge](#)

Software prerequisites

- **Kali Linux** --> Downloadable [here](#)

Note: Ambient IT does not own OSCP™; this certification belongs to OffSec® Services LLC.

OUR OSCP™ CERTIFICATION TRAINING PROGRAM

Introduction & Useful Tools

- All About OSCP
 - Prerequisites
 - Objectives
 - Exam
 - Training Content
 - Available resources
 - PEN-200 Lab
- The pentester's Swiss Army knife
 - Useful tools
 - Bind shells
 - Reverse shells

Reconnaissance

- IT system mapping
- Passive discovery (OSINT)
- Active discovery phase
- DNS enumeration
- Zone transfer
- Port scanning
- Service enumeration
 - SSL/TLS scan
- WAF detection

Web attacks

- Useful tools
 - URL fuzzing
 - Web attack proxies
 - Web scanners
- SQL injections
 - Manual exploitation of UNION/error-based SQL injections
 - Automation of complex SQL injection exploitation: blind / time-based
 - Exfiltration of sensitive data & Takeover of the underlying system
- Cross-Site Scripting (XSS)
- Path traversal
- Exploitation of RCE (Remote Code Execution) vulnerabilities
 - File upload forms
 - System command injection

Public exploits

- Fingerprinting and identification of third-party software and service versions
- Analysis and execution of public exploit code
- Modification and adaptation of exploits based on context

Post-exploitation

- Upgrading a shell
- Transferring files to the compromised server
- Taking full control of the server
 - Privilege escalation techniques
 - Become an "Administrator" (Windows) or "root" (Linux)
- Information exfiltration
- Pivoting and bouncing (indirect attack on an inaccessible network)

Active Directory

- ActiveDirectory compromise methodology
- ActiveDirectory enumeration
- Brute force and dictionary attacks
- Compromise paths
- Lateral movement techniques

PowerShell Empire

- Listeners and stagers
- Empire for the post-exploitation phase
- ActiveDirectory compromise with Empire

Bonus

- Practical exercise: compromising an ActiveDirectory domain
- Review of any points that may still be unclear (depending on participants' needs)

Target companies

This training is intended for both individuals and companies, large or small, wishing to train their teams in new advanced IT technology or to acquire specific professional knowledge or modern methods.

Positioning at the start of training

The positioning at the start of the training complies with Qualiopi quality criteria. Upon final registration, the learner receives a self-assessment questionnaire that allows us to assess their estimated level of knowledge of different types of technologies, their expectations and personal objectives for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could be problematic for the monitoring and smooth running of the training session.

Teaching methods

Practical training: 60% practical, 40% theory. Training materials distributed in digital format

to all participants.

Organization

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

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been correctly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training course.