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

Updated 03/02/2025

Sign up

OSCP™ training (PEN-200)

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

5 days (35 hours)

PRESENTATION

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

Highly recognized on the market, this certification will prove your skills in ethical hacking. You'll know how to perform pentests in a methodical and advanced way.

This comprehensive OSCP™ training course help you improve your IT security knowledge and be able to find the most complex security flaws.

All the security flaws present in the exam will be discussed, such buffer overflows, web and Active Directory attacks.

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

Once you've completed our bootcamp-style coaching (one half-day training session per week for 2 months), you'll be eligible for certification.

Training content

- 90-day self-study access to the Labs
- 10 expert support sessions: 10 x Monday mornings (9am-12.30pm) per week (35 hours)
- 1 certification pass
- Access to the learners' forum

OBJECTIVES

- Understand the main vulnerabilities and intrusion techniques for systems and the web
- Be able to enter a realistic network by putting it into practice on the lab
- Develop your pentesting skills with the "Try harder" method
- Obtain OffSec Certified Professional (OSCP) certification

TARGET AUDIENCE

- Ethical hackers
- IT security expert
- Developers
- Technical architects
- Directors
- Project managers
- Reconverted to IT security

Prerequisites

- Knowledge :
  - TCP/IP networks - Intermediate
  - Linux/Windows administration - Intermediate
  - Scripting Bash/Python - Basic
- Fluency in technical English
- Minimum personal investment of 2 hours per day to carry out the labs
- Refer to the technical requirements for taking part in the supervised test
- Test My Knowledge

Software requirements

- **Kali Linux** --> Download here

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

OSCP™ CERTIFICATION TRAINING PROGRAM

Introduction & Useful tools

- All about OSCP
  - Prerequisites
  - Objectives
  - Review
  - Training content
  - Available resources
  - Lab PEN-200
- The pentester's Swiss Army knife
  - Useful tools
  - Bind shells
  - Reverse shells

Recognition

- IS mapping
- Passive discovery (OSINT)
- Active" discovery phase
- DNS enumeration
- Zone transfer
- Port scanning
- List of services
- Scan SSL/TLS
- WAF detection

Web attacks

- Useful tools
  - Fuzzing URLs
  - Web attack proxies
  - Web scanners
- SQL injections
  - Manual exploitation of UNION / error-based SQL injections
  - Automated exploitation of complex SQL injections: blind / time-based
  - Exfiltration of sensitive data & Taking control of the underlying system
- Cross-Site Scripting (XSS)
- Path Traversal
- Exploitation of RCE (Remode Code Execution) vulnerabilities
  - File upload forms
  - System command injection

Public exploits

- Fingerprinting and version identification for third-party software and services
- Analysis and implementation of public operating codes
- Context-sensitive modification and adaptation of exploits

Post Operation

- Upgrading a shell
- File transfer to compromised server
- Total server control
  - Privilege elevation techniques
  - Become "Administrator" (Windows) or "root" (Linux)
- Exfiltration of information
- Pivoting and rebound (indirect attack on an inaccessible network)

Active Directory

- ActiveDirectory compromise methodology
- ActiveDirectory enumeration
- Brute force and dictionary attacks
- Paths of compromise
- Lateral movement techniques

PowerShell Empire

- Listeners and staggers
- Empire for the post-operation phase
- ActiveDirectory compromise with Empire

Bonus

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

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 training: 60% Practical, 40% Theory. Training material distributed in

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 verifies the correct acquisition of skills.

Sanction

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