AMBIENT-IT

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

Updated 03/15/2024

Sign up

OSEP™ Certification Training

ALL-IN-ONE: EXAM INCLUDED IN PRICE WITH PEN-300 COURSE

OFFSEC CERTIFICATIONS - BUY YOUR CERTIFICATIONS

4 days (28 hours)

PRESENTATION

Do you have OSCP™ certification, and want to master the most advanced penetration techniques? OSEP™ certification will enable you to prove your expertise in pentesting against hardened systems.

This OSEP™ training course will teach you how to identify intrusion opportunities and methodically execute complex penetration tests.

This OSEP™ training course will cover all the elements present during the exam, such as Client Side Code Execution, antivirus evasion and the Microsoft SQL attack.

After completing our preparation, you'll be able to take the OSEP™ certification.

THE PREMIUM PACK

- 90 days' access to self-training Labs
- 8 expert coaching sessions: 8 x Monday mornings (9am-12.30pm) per week (28 hours)
- 1 Passage to certification

OBJECTIVES

- Mastering intrusion techniques such as client-side attacks and ways of bypassing antivirus and identification systems
- Know how to conduct penetration tests in a methodical and advanced manner

- How to carry out penetration tests against organizations with enhanced security systems

TARGET AUDIENCE

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

Prerequisites

- Possess OSCP™ certification
- How to use the Linux terminal
- Basic knowledge of Bash, Python and PowerShell
- Good knowledge of penetration testing

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

OSEP™ CERTIFICATION TRAINING PROGRAM

Client-side attack with Microsoft Office

- Create a dropper
- HTML Smuggling
- Phishing with Microsoft Office
- Phishing PreTexting
- Running Shellcode on Word
- PowerShell Shellcode Runner

Client-side attack with Windows Script Host

- Creating a dropper with Javascripts
- Javascript meterpreter dropper
- DotNetToJscript
- Calling the Win32 API from C#
- Shellcode Runner in C#
- Javascript Shellcode Runner
- SharpShooter

Active Directory operation

- Safety permits
- Kerberos delegation
- The Active Directory forest
- Controlling the forest
- Active Directory approval relationships between forests
- Compromising a new forest

Microsoft SQL attack

- Microsoft SQL Enumeration
- Microsoft SQL Authentication
- UNC Path Injection
- Microsoft SQL Escalation
- Linked SQL servers

Antivirus evasion

- Antivirus overview
- Simulate the target environment
- Find Signatures
- Bypassing antivirus software with Metasploit
- Bypassing antivirus software with C#
- Playing with our behavior
- Bypassing antivirus software on Microsoft Office
- Hiding PowerShell on VBA
- Introduction to WinDbg
- Antimalware scan interface
- Sabotaging antimalware scans with PowerShell
- Bypassing JavaScript anti-malware scans

Process Injection and Migration

- Presentation of the Injection and Migration Process
- Process Injection with C#
- DLL injection
- Reflective DLL injection
- Process Hollowing

Bypassing network filters

- DNS filters
- Web proxies
- IDS and IPS sensors
- Complete package capture devices
- HTTPS inspection
- Domain Fronting
- DNS Tunneling

Application Whitelisting

- Whitelisting Application overview
- Basic bypass
- AppLocker bypass with PowerShell
- AppLocker bypass with C#
- Bypassing AppLocker with JavaScript

Lateral movement on Windows and Linux

- Remote Desktop Control
- Fileless lateral movement
- Lateral movement with SSH
- Attacking Ansible
- Kerberos on Linux

Linux Post-Exploitation

- User configuration files
- Bypassing antivirus software
- Shared libraries

FAQ - QUESTIONS / ANSWERS

WHAT CONTENT WILL I RECEIVE FOR OSEP™ TRAINING?

In addition to the preparation we offer. OSEP™ training includes all training materials issued by OffSec:

- Over 19 hours of video training
- A 700-page training book in pdf format
- Access to the learners' forum
- Access to the lab for 60 to 90 days, depending on the package chosen

HOW DOES THE OSEP™ CERTIFICATION EXAM WORK?

You must read the official guide before taking your exam.

The practical phase of the exam lasts 47 hours and 45 minutes, and involves attacking as many machines as possible. After this phase, you'll have another 24 hours to complete and send in the operations report explaining your approach.

IN WHICH LANGUAGE IS THE OSEP™ TRAINING TAUGHT?

Exam preparation will be in French. However, the additional content offered by OffSec is in English.

IS THE OSEP™ CERTIFICATION EXAM INCLUDED IN THE COURSE PRICE?

Yes, you can take the exam after completing the training course. HOW

LONG IS THE LAB AVAILABLE FOR?

You have access to the lab for 60 to 90 days, depending on the package

you choose. IN WHICH LANGUAGE IS THE EXAM HELD?

The exam is conducted in English.

DO I NEED A WEBCAM?

Yes, your webcam must be active throughout your entire exam, and be able to film your entire room.

DO I NEED A GOOD INTERNET CONNECTION?

Yes, because your computer has to support a TeamViewer stream for 24 hours, while constantly attacking other machines.

What's the difference between Offensive Security and Offsec?

Since March 2023, Offensive Security has been renamed OffSec. It is the same organization.

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 confirmed, 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 with regard to the training to come, within the limits imposed by the format selected. This

The questionnaire also enables us to anticipate any connection or internal security problems (intra-company or virtual classroom) that 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.