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

Updated 04/11/2024

Sign up

OSWP™ Certification Training

ALL-IN-ONE: EXAM INCLUDED IN PRICE WITH PEN-210 COURSE

OFFSEC CERTIFICATIONS - BUY YOUR CERTIFICATIONS

4 days (28 hours)

PRESENTATION

OSWP™ certification will prove your expertise in auditing and securing wireless devices. This OSWP™ training will enable you to identify existing encryptions and security loopholes on 802.11 networks. You'll then be able to bypass network security restrictions and recover encryption keys.

This OSWP™ training will cover all the elements present during the exam such as cracking in various forms, bypassing WEP shared key authentication the use of Rogue Access Point....

You'll be able to retrieve wireless information, bypass access restrictions, crack various WEP, WPA and WPA2 implementations and conduct MITM attacks.

After completing our preparation, you'll be able to pass the OSWP™ certification included in the fee.

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

- A better understanding of wireless device safety
- Execute advanced attacks such as PRGA key extraction and one-way packet injection
- How to set up attacks against WEP and WPA encrypted networks
- Master the tools of the BackTrack suite

TARGET AUDIENCE

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

Prerequisites

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

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

OSWP™ CERTIFICATION TRAINING PROGRAM

Wireless network and IEEE 802.11 operation

- Introduction to IEEE 802.11
- Standards and amendments
- The 802.11 protocol
- Network infrastructure
- Ad-Hoc Network
- Wireless Distribution System
- Monitor mode
- Wireless Linux stacks and drivers
- Wireless recognition
- Airgraph-ng
- Kismet
- GISKismet
- Wireless Reconnaissance Lab

Choosing your equipment

- Adapter types
- dB, dBm, dBi, mW, W
- Choosing your wireless card
- Choosing your antenna

Packages and frames

- Wireless packages - 802.11 MAC Frame
- Control frames
- Managing frames
- Frame data
- Interacting with networks

WEP cracking

- Airmon-ng
- Airodump-ng
- Aireplay-ng false authentication attack
- Fake Authentication Lab
- Aireplay-ng deauthentication attack
- Aireplay-ng ARP Request Replay Attack
- Aircrack-ng
- Cracking WEP via a client
- Attack Aireplay-ng Interactive Packet Replay
- Crack the WEP key
- Crack clientless WEP networks
- Aireplay-n fragmentation attack
- Packetforge-ng
- Attack Aireplay-ng KoreK ChopChop
- Attack Aircrack-ng Interactive Packet Replay
- WEP Cracking without Lab client
- Bypass shared WEP authentication key

WPA and WPA2 cracking

- Crack WPA/WPA2 PSK with Aircrack-ng
- Aireplay-ng deauthentication attack
- Aircrack-ng and WPA
- Airolib-ng
- Crack WPA with JTR and Aircrack-ng
- Using Aircrack-ng with John the Ripper
- John the Ripper Lab
- Crack WPA with coWPAtty
- coWPAtty Dictionary Mode
- coWPAtty Rainbow Table Mode
- coWPAtty Lab
- Crack WPA with Pyrit

- Pyrit Dictionary Attack
- Pyrit Database Mode
- Pyrit Lab

Rogue Access Points

- Airbase-ng
- Karmetasploit
- MITM attack
- Rogue Access Points Lab

FAQ - QUESTIONS / ANSWERS

WHAT CONTENT WILL I RECEIVE FOR OSWP™ TRAINING?

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

- 3.5 hours of video training
- A 380-page training book in pdf format
- Access to the learners' forum
- Lab access

IN WHICH LANGUAGE IS THE OSWP™ TRAINING TAUGHT?

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

IS THE OSWP™ 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'll set up your own lab. It will be accessible at all times. HOW DOES THE

OSWP™ CERTIFICATION EXAM WORK?

The OSWP™ exam lasts 4 hours and requires you to connect to the dedicated lab via SSH. You'll need to perform wireless information gathering and various attacks to gain access to networks. You must also submit a full penetration test report.

WHAT LANGUAGE IS USED FOR THE EXAM?

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 4 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.

How much does certification cost?

The price of this certification is $1649.

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 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.