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

Mis à jour le 11/04/2024

S'inscrire

# Formation Certification OSWP™

ALL-IN-ONE : EXAMEN INCLUS AU TARIF AVEC LE COURS PEN-210

CERTIFICATIONS OFFSEC - ACHETER VOS CERTIFICATIONS

4 jours (28 heures)

## PRÉSENTATION

La certification OSWP™ prouvera votre expertise en audit et en sécurisation des appareils sans fils. Cette formation OSWP™ vous permettra de pouvoir identifier les cryptages et les failles de sécurité existantes sur les réseaux 802.11. Vous pourrez alors contourner les restrictions de sécurité du réseau et récupérer les clés de cryptage.

Cette formation OSWP™ couvrira tous les éléments présents lors de l'examen comme le cracking sous diverse formes, le contournement de l'authentification par clé partagée WEP l'utilisation du Rogue Access Point...

Ainsi, vous saurez récupérer des informations sans fil, contourner les restrictions d'accès, cracker diverses implémentations WEP, WPA et WPA2 ou encore conduire des attaques de type « MITM ».

Après avoir suivi notre préparation, vous serrez en mesure de passer la certification OSWP™ incluse au tarif.

## LE PACK PREMIUM

- 90 jours d'accès aux Labs en autoformation
- 8 accompagnements d’expert : 8 x lundi matin (de 9h à 12h30) par semaine (28 heures)
- 1 Passage de la certification

## OBJECTIFS

- Une meilleure compréhension de la sécurité des appareils sans fils
- Exécuter des attaques avancées telles que l'extraction de clés PRGA et l'injection unidirectionnelle de paquets
- Savoir mettre en place des attaques contre les réseaux cryptés WEP et WPA
- Maîtriser le outils de la suite BackTrack

# PUBLIC VISÉ

- Hackers éthiques
- Expert en sécurité informatique
- Développeurs
- Architectes techniques
- Administrateurs
- Chefs de projet

# Pré-requis

- Savoir utiliser le terminal Linux
- Connaissance de base en Bash, Python et PowerShell
- Bonne connaissance en test de pénétration

Note : Ambient IT n’est pas propriétaire de OSWP™ cette certification appartient à OffSec ® Services LLC.

# PROGRAMME DE NOTRE FORMATION CERTIFICATION OSWP™

## Fonctionnement du réseau sans fil et de l'IEEE 802.11

- Introduction à IEEE 802.11
- Les normes et les amendements
- Le protocole 802.11
- Infrastructure réseau
- Réseau Ad-Hoc
- Wireless Distribution System
- Mode moniteur
- Stacks et Drivers Linux sans fil
- Reconnaissance sans fil
- Airgraph-ng
- Kismet
- GISKismet
- Wireless Reconnaissance Lab

## Choisir son matériel

- Les types d'adaptateurs
- dB, dBm, dBi, mW, W
- Choisir sa carte sans fil
- Choisir son antenne

## Paquets et frames

- Paquets sans fil - 802.11 MAC Frame
- Contrôler les frames
- Gérer les frames
- Les données frames
- Interagir avec les réseaux

## WEP cracking

- Airmon-ng
- Airodump-ng
- Attaque en fausse authentification Aireplay-ng
- Fake Authentication Lab
- Attaque Aireplay-ng de déseauthentification
- Aireplay-ng ARP Request Replay Attack
- Aircrack-ng
- Cracker le WEP via un client
- Attaque Aireplay-ng Interactive Packet Replay
- Cracker la clé WEP
- Cracker les réseaux WEP sans client
- Attaque de fragmentation Aireplay-n
- Packetforge-ng
- Attaque Aireplay-ng KoreK ChopChop
- Attaque Aircrack-ng Interactive Packet Replay
- WEP Cracking sans client Lab
- Contourner la clé d'authentification WEP partagée

## WPA et WPA2 cracking

- Cracker WPA/WPA2 PSK avec Aircrack-ng
- Attaque Aireplay-ng de déseauthentification
- Aircrack-ng et WPA
- Airolib-ng
- Cracker WPA avec JTR et Aircrack-ng
- Utiliser Aircrack-ng avec John the Ripper
- John the Ripper Lab
- Cracker WPA avec coWPAtty
- coWPAtty Dictionary Mode
- coWPAtty Rainbow Table Mode
- coWPAtty Lab
- Cracker WPA avec Pyrit

- Pyrit Dictionary Attack
- Pyrit Database Mode
- Pyrit Lab

## Rogue Access Points

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

## FAQ – QUESTIONS / RÉPONSES

### QUEL CONTENU VAIS-JE RECEVOIR POUR LA FORMATION OSWP™ ?

En plus de la préparation que nous proposons. La formation OSWP™ comprend tous les supports de formation délivrés par OffSec :

- 3,5 heures de formation vidéos
- Un livre de formation en format pdf de 380 pages
- Accès au forum des apprenants
- Accès au lab

### DANS QUELLE LANGUE LA FORMATION OSWP™ VOUS EST ENSEIGNÉE ?

La préparation à l'examen sera en français. Cependant, les contenus supplémentaires proposés par OffSec sont en anglais.

### L'EXAMEN POUR LA CERTIFICATION OSWP™ EST-ELLE COMPRIS DANS LE PRIX DE LA FORMATION ?

Oui, vous pourrez passer l'examen après avoir suivi la formation.

### POUR QUELLE DURÉE LE LAB EST-IL ACCESSIBLE ?

Vous installerez votre propre lab. Il sera accessible à tout moment.

### COMMENT SE DÉROULE L'EXAMEN POUR LA CERTIFICATION OSWP™ ?

L'examen OSWP™ dure 4 heures et nécessite que vous vous connectiez au lab dédié via SSH. Vous devrez effectuer une collecte d'informations sans fil et diverses attaques pour accéder aux réseaux. Vous devez également soumettre un rapport de test de pénétration complet.

### EN QUELLE LANGUE SE DÉROULE L'EXAMEN ?

L'examen se déroule en anglais.

### DOIS-JE POSSÉDER UNE WEBCAM ?

Oui, votre webcam doit être active durant la totalité de votre examen, elle doit pouvoir filmer toute votre pièce.

DOIS-JE AVOIR UNE BONNE CONNEXION INTERNET ?

Oui, car votre ordinateur doit supporter pendant 4h un flux TeamViewer tout en attaquant en permanence des machines.

Quelle est la différence entre Offensive Security et OffSec ?

Depuis mars 2023, l'entité Offensive Security s'est renommée en OffSec. Il s'agit du même organisme.

Quel est le prix de la certification ?

Le prix de cette certification est de 1649 $

## Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

## Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

## Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

## Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

## Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

## Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.