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

Mis à jour le 15/03/2024

S'inscrire

Formation Certification OSEP™

ALL-IN-ONE : EXAMEN INCLUS AU TARIF AVEC LE COURS PEN-300

CERTIFICATIONS OFFSEC - ACHETER VOS CERTIFICATIONS

4 jours (28 heures)

PRÉSENTATION

Vous avez la certification OSCP™, et vous souhaitez maîtriser les techniques de pénétration les plus avancées ? La certification OSEP™ vous permettra de prouver votre expertise en pentesting contre des systèmes renforcés.

Cette formation OSEP™ vous permettra de savoir comment identifier les opportunités d'intrusion et comment exécuter méthodiquement des tests de pénétrations complexes.

Cette formation OSEP™ couvrira tous les éléments présents lors de l'examen comme le Client Side Code Execution, l'évasion aux antivirus ou encore l'attaque Microsoft SQL.

Après avoir suivi notre préparation, vous pourrez passer la certification OSEP™.

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

- Maîtriser les techniques d'intrusion comme les attaques côté client et les moyens de contourner les antivirus et les identifications
- Savoir comment conduire des tests de pénétration de manière méthodique et avancée

- Savoir entreprendre des tests de pénétration contre des organisations ayant un système de sécurité renforcé

PUBLIC VISÉ

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

Pré-requis

- Posséder la certification OSCP™
- 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 OSEP™ cette certification appartient à OffSec ® Services LLC.

PROGRAMME DE NOTRE FORMATION CERTIFICATION OSEP™

Attaque côté client avec Microsoft Office

- Créer un dropper
- HTML Smuggling
- Phishing avec Microsoft Office
- Phishing PreTexting
- Executer Shellcode sur Word
- PowerShell Shellcode Runner

Attaque côté client avec Windows Script Host

- Créer un dropper avec Javascripts
- Javascript meterpreter dropper
- DotNetToJscript
- Appel de l'API de Win32 à partir de C#
- Shellcode Runner in C#
- Javascript Shellcode Runner
- SharpShooter

Exploitation de l'Active Directory

- Les Permissions de sécurité
- Délégation Kerberos
- La forêt Active Directory
- Contrôler la forêt
- Les relations d'approbation Active Directory entre les forêts
- Compromettre une nouvelle forêt

Attaque Microsoft SQL

- Microsoft SQL Enumération
- Microsoft SQL Authentication
- UNC Path Injection
- Escalade Microsoft SQL
- Serveurs SQL liés

Evasion d'antivirus

- Présentation des antivirus
- Simuler l'environnement cible
- Trouver les Signatures
- Contourner les antivirus avec Metasploit
- Contourner les antivirus avec C#
- Jouer avec notre comportement
- Contourner les antivirus sur Microsoft Office
- Cacher PowerShell sur VBA
- Introduction à WinDbg
- Interface des scans antimalware
- Saboter les scans antimalware avec PowerShell
- Contourner les scans antimalware JavaScript

Process Injection et Migration

- Présentation du Process Injection et Migration
- Process Injection avec C#
- Injection DLL
- Injection DLL réfléchie
- Process Hollowing

Contourner les filtres réseaux

- Filtres DNS
- Proxies web
- Capteurs IDS et IPS
- Appareils de capture de paquets complets
- Inspection HTTPS
- Domain Fronting
- DNS Tunneling

Application Whitelisting

- Présentation de l'Application Whitelisting
- Contournement basique
- Contournement AppLocker avec PowerShell
- Contournement AppLocker avec C#
- Contournement AppLocker avec JavaScript

Mouvement laléral sur Windows et Linux

- Remote Desktop Control
- Mouvement latéral de type fileless
- Mouvemnt latéral avec SSH
- Attaquer Ansible
- Kerberos sur Linux

Linux Post-Exploitation

- Fichiers de configuration de l'utilisateur
- Contourner l'antivirus
- Bibliothèques partagées

FAQ – QUESTIONS / RÉPONSES

QUEL CONTENU VAIS-JE RECEVOIR POUR LA FORMATION OSEP™ ?

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

- Plus de 19 heures de formation vidéos
- Un livre de formation en format pdf de 700 pages
- Accès au forum des apprenants
- Accès au lab pendant 60 à 90 jours selon la formule choisie

COMMENT SE DÉROULE L'EXAMEN POUR LA CERTIFICATION OSEP™ ?

Vous devez absolument lire le guide officiel avant de passer votre examen.

La phase pratique de l'examen dure 47 heures et 45 minutes, cette phase consiste à attaquer le maximum de machines. Après cette phase, vous aurez à nouveau 24 heures pour compléter et envoyer le rapport d'exploitation où vous expliquerez votre démarche.

DANS QUELLE LANGUE LA FORMATION OSEP™ 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 OSEP™ EST-IL 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 avez accès au lab pendant 60 à 90 jours selon la formule choisie.

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 24h 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.

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.

Organisme de formation enregistré sous le numéro 11 75 54743 75. Cet enregistrement ne vaut pas agrément de l’État.
© Ambient IT 2015-2024. Tous droits réservés. Paris, France - Suisse - Belgique - Luxembourg