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

Mis à jour le 03/02/2025

S'inscrire

Formation OSCP™ (PEN-200)

ALL-IN-ONE : EXAMEN INCLUS AU TARIF AVEC LE COURS PEN-200

5 jours (35 heures)

PRÉSENTATION

Maintenir ses infrastructures sécurisées contre les attaques cybercriminelles est devenu impératif. OSCP™ est la certification d'OffSec la plus célèbre.

Très reconnue sur le marché, cette certification prouvera vos compétences en hacking éthique. Vous saurez ainsi comment effectuer des pentests de manière méthodique et avancée.

Cette formation complète OSCP™ vous permettra d'améliorer vos connaissances en sécurité informatique et pouvoir trouver les failles de sécurité les plus complexes.

Toutes les failles de sécurités présentes lors de l'examen seront évoquées comme les dépassements de tampon, les attaques web et Active Directory.

Vous apprendrez à maîtriser le pentesting avec Kali Linux, l'une des distributions Linux les plus populaires lorsqu'il s'agit de tests d'intrusion.

Après avoir suivi notre programme d'accompagnement de type bootcamp (une demi-journée de formation par semaine pendant 2 mois), vous pourrez prétendre au passage de la certification.

Contenu de la formation

- 90 jours d'accès aux Labs en autoformation
- 10 accompagnements d'expert : 10 x lundi matin (de 9h à 12h30) par semaine (35 heures)
- 1 passage à la certification
- Accès au forum des apprenants

OBJECTIFS

- Connaître les principales vulnérabilités et techniques d'intrusion système / web
- Être capable de s'introduire sur un réseau réaliste en mettant en pratique sur le lab
- Développer ses compétences en pentest avec la méthode "Try harder"
- Obtenir la certification OffSec Certified Professional (OSCP)

PUBLIC VISÉ

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

Pré-requis

- Connaissances :
  - Réseaux TCP/IP - Intermédiaire
  - Administration Linux/Windows - Intermédiaire
  - Scripting Bash/Python - Basique
- Maîtrise de l'anglais technique
- Investissement personnel minimal de 2h par jour pour réaliser les labs
- Se référer aux exigences techniques pour participer à l'examen surveillé
- Tester Mes Connaissances

Pré-requis logiciels

- **Kali Linux** --> Téléchargeable ici

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

PROGRAMME DE NOTRE FORMATION CERTIFICATION OSCP™

Introduction & Outils utiles

- Tout sur l'OSCP
  - Prérequis
  - Objectifs
  - Examen
  - Contenu de la formation
  - Ressources à disposition
  - Lab PEN-200
- Le couteau suisse du pentester
  - Outils utiles
  - Bind shells
  - Reverse shells

Reconnaissance

- Cartographie du SI
- Découverte passive (OSINT)
- Phase de découverte "active"
- Énumération DNS
- Transfert de zone
- Scan de ports
- Énumération de services
- Scan SSL/TLS
- Détection de WAF

Attaques web

- Outils utiles
  - Fuzzing URL
  - Proxys d'attaque web
  - Scanners web
- Injections SQL
  - Exploitation manuelle d'injections SQL de type UNION / error-based
  - Automatisation d'exploitation d'injections SQL complexes : blind / time-based
  - Exfiltration de données sensibles & Prise de contrôle du système sous-jacent
- Cross-Site Scripting (XSS)
- Path Traversal
- Exploitation de vulnérabilités RCE (Remode Code Execution)
  - Formulaires d'upload de fichiers
  - Injection de commandes systèmes

Exploits publics

- Fingerprinting et identification de la version des logiciels et services tiers
- Analyse et exécution de codes d'exploitation publics
- Modification et adaptation d'exploits en fonction du contexte

Post Exploitation

- Upgrader un shell
- Transfert de fichiers vers le serveur compromis
- Prise de contrôle total du serveur
  - Techniques d'élévation de privilèges
  - Devenir « Administrateur » (Windows) ou « root » (Linux)
- Exfiltration d'informations
- Pivoting et rebond (attaque indirecte d'un réseau inaccessible)

Active Directory

- Méthodologie de compromission ActiveDirectory
- Énumération ActiveDirectory
- Attaques par force brute et par dictionnaire
- Chemins de compromission
- Techniques de mouvement latéral

PowerShell Empire

- Listeners et staggers
- Empire pour la phase post-exploitation
- Compromission d'ActiveDirectory avec Empire

Bonus

- TP : compromission d'un domaine ActiveDirectory
- Revue des points qui seraient éventuellement encore flous (en fonction des besoins des participants)

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.