

Certifiante

Formation Certified Lead Ethical Hacker, avec certification PECB

Réf. SF34469

Développez une expertise opérationnelle en tests d'intrusion, de la reconnaissance au reporting, dans un cadre légal et conforme aux bonnes pratiques !

5 j
Durée

4 250 € HT
Inter / participant

0
Sessions à venir

Objectifs pédagogiques

- ✓ Maîtriser les concepts, méthodes et techniques utilisés par les organisations de cybersécurité et les ethical hackers pour réaliser des tests d'intrusion
- ✓ Acquérir une vision complète des composants et du fonctionnement des activités d'ethical hacking
- ✓ Comprendre les liens entre les méthodologies de pentest, les cadres réglementaires et les normes applicables

Public visé & prérequis

Public visé Responsables de la sécurité des systèmes d'information (RSSI), Tous

Prérequis Avoir une bonne connaissance des principes et concepts de la sécurité de l'information ainsi que des compétences avancées sur les systèmes d'exploitation. Il est recommandé de disposer de notions en réseaux informatiques et des bases de programmation.

Programme détaillé

Jour 1 – Introduction à l'ethical hacking

Fondamentaux et cadre de l'ethical hacking
Principes, périmètre et approche d'un test d'intrusion

Jour 2 – Lancement de la phase de reconnaissance

Collecte d'informations : méthodes et bonnes pratiques
Outils et techniques de reconnaissance

Jour 3 – Lancement de la phase d'exploitation

Identification des vulnérabilités et préparation de l'attaque
Techniques d'exploitation en environnement contrôlé

Jour 4 – Post-exploitation et restitution

Post-exploitation : élévation de privilèges, pivot, transferts de fichiers
Structuration des preuves et rédaction du rapport
Recommandations et présentation des résultats

Jour 5 – Examen de certification

Passage de l'examen PECB Certified Lead Ethical Hacker
L'examen « PECB Certified Lead Ethical Hacker » est conforme aux exigences du programme PECB (ECP) et couvre les domaines de compétences suivants :
– Outils et techniques de collecte d'informations
– Modélisation des menaces et identification des vulnérabilités

- Techniques d'exploitation
- Élévation de privilèges
- Pivot et transferts de fichiers
- Reporting

L'évaluation comprend deux volets : une partie pratique (compromettre au moins deux machines cibles dans le cadre d'un pentest) et une partie rédactionnelle (rapport documentant la démarche et les résultats). L'examen est open book : les supports de formation et notes personnelles sont autorisés.

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Cybersécurité et Protection des Données : 4,9/5 — 13 avis

William B. — Prévoir l'envoi à chaque participant du livre de CISS au moins un mois avant la formation.

Mickael L. — il est top Romain GARCIA

Votre formateur

Bechir S. — Formateur Sécurité Offensive & Red Team

Bechir intervient sur des formations portant sur la sécurité offensive, le Red Team et le pentest. Parmi les formations qui lui sont confiées figure notamment « Certified Lead Ethical Hacker,... »

Ils nous font confiance

Cette année notre filière Cybersécurité et Protection des Données a accompagné plus de 69 entreprises dont :

AVEM MÉTROPOLE DE LYON ACTIMAGE CONSULTING SAS ADISTA ADVENTIEL AIGA ALCYOR ALDORIA ALSTOM ALTEN SA +59 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com