

Lead Ethical Hacker (CLEH) : expert en piratage éthique et tests d'intrusion

Code CLEH

4,5 jours

31 heures

 Tarifs & Sessions Certification incluse Labs inclus Formateurs certifiés Cours officiel Take2

DESCRIPTION

Face à la multiplication des cyberattaques, le **hacking éthique** est devenu l'une des disciplines les plus stratégiques pour protéger les systèmes d'information en entreprise. Maîtriser les techniques de piratage éthique et de tests d'intrusion est une nécessité pour tout professionnel souhaitant **se spécialiser dans la sécurité offensive**.

Cette **formation de 4,5 jours** vous dote des compétences et des connaissances nécessaires pour mener des opérations avancées en hacking éthique et en **tests d'intrusion** sur des systèmes d'information et des infrastructures réseau. Elle inclut des **labs pratiques sur machine virtuelle**, accessibles via navigateur, et des études de cas simulant un test d'intrusion réel de bout en bout.

Au terme de ce programme, vous serez prêt à passer l'**examen officiel PECB Lead Ethical Hacker**, compris dans notre offre. Cet examen pratique en ligne qui requiert de compromettre 3 machines cibles vous permettra d'obtenir la certification **PECB Certified Lead Ethical Hacker** (en savoir plus dans l'onglet certification).

POINTS FORTS

- **Support de cours complet** : plus de 450 pages de documentation officielle PECB, disponible en français.
- **Labs pratiques sur machine virtuelle** : environnement virtuel dédié accessible via navigateur pour s'entraîner sur des scénarios réels de bout en bout.
- **35 crédits CPD** : une attestation de fin de formation valorisant 35 crédits de développement professionnel continu (Continuing Professional Development).
- **Examen PECB inclus** : le passage de l'examen officiel est compris dans notre offre, sans frais supplémentaires.
- **Retake gratuit** : en cas d'échec à l'examen, vous pouvez le repasser gratuitement dans les 12 mois.

PUBLIC VISÉ

Cette formation s'adresse aux professionnels expérimentés en sécurité de l'information souhaitant maîtriser les techniques de hacking éthique et de tests d'intrusion. Le public inclut notamment :

- les **professionnels et auditeurs cybersécurité** qui souhaitent maîtriser les méthodes de hacking éthique et les techniques avancées de tests d'intrusion ;
- les **responsables SSI et experts consultants** qui souhaitent comprendre et gérer des opérations de piratage éthique au sein de leur organisation ;
- les **administrateurs systèmes et réseaux** qui souhaitent apprendre à planifier, exécuter et documenter des tests d'intrusion professionnels.

OBJECTIFS

À l'issue de cette formation Lead Ethical Hacker, vous atteindrez les objectifs de compétences suivants :

- maîtriser les concepts, méthodes et techniques employés pour conduire des tests d'intrusion sur des systèmes d'information et des infrastructures réseau ;
- collecter des informations sur les cibles et identifier les vulnérabilités avec les outils de reconnaissance appropriés ;
- modéliser les menaces et élaborer des scénarios d'attaque adaptés au périmètre défini ;
- comprendre les synergies entre les méthodes de tests d'intrusion, les normes et les réglementations en vigueur ;
- compromettre des systèmes cibles dans un environnement virtuel contrôlé et documenter le processus dans un rapport professionnel ;
- se préparer et réussir l'examen technique PECB Certified Lead Ethical Hacker.

PRÉREQUIS

Suivre cette formation nécessite les prérequis suivants :

- **Compétences techniques** : maîtriser les concepts et principes de la sécurité de l'information et posséder des compétences avancées en administration de systèmes d'exploitation (Windows et Linux).
- **Bases théoriques** : avoir de bonnes connaissances en réseaux informatiques (TCP/IP, protocoles, architecture) et en techniques de programmation.

PROGRAMME DÉTAILLÉ

Jour 1 : découvrir les fondamentaux du hacking éthique

- Les objectifs et le déroulement de la formation.
- Les normes, méthodes et outils de test d'intrusion.
- Les principes de base du hacking éthique.
- Les fondamentaux du réseautage et de la cryptographie.
- Les nouvelles tendances et technologies en matière de hacking.
- Les fondamentaux de Kali Linux.
- La mise en place et l'analyse de la portée d'un test d'intrusion.
- Les aspects légaux et les accords contractuels.

LABS

- Prise en main de l'environnement virtuel PECB et configuration de Kali Linux pour les tests d'intrusion.

Jour 2 : initier la phase de reconnaissance

- La reconnaissance passive.
- La reconnaissance active.
- L'identification des vulnérabilités.

LABS

- Effectuer une reconnaissance passive et active sur une machine virtuelle cible et cartographier les vulnérabilités identifiées.

Jour 3 : conduire la phase d'exploitation

- Le modèle de menace et la stratégie d'attaque.
- Le contournement des systèmes de détection d'intrusion (IDS).
- Les attaques côté serveur et côté client.
- Les attaques provenant des infrastructures web.
- Les attaques par les réseaux sans fil (Wi-Fi).
- L'escalade des droits, le pivoting réseau et les transferts de fichiers.
- La conservation des accès.

LABS

- Exploiter une vulnérabilité identifiée sur une machine virtuelle cible, escalader les droits et maintenir l'accès.

Jour 4 : assurer la post-exploitation et rédiger le rapport

- Le nettoyage et la suppression des artefacts.
- Le compte rendu des résultats.
- Les conseils pour atténuer les failles de sécurité détectées.

LABS

- Réaliser la phase de post-exploitation sur l'environnement virtuel cible et rédiger un rapport de test d'intrusion professionnel.

Jour 5 (demi-journée) : préparer l'examen PECB CLEH

- Révision des concepts clés et des compétences acquises tout au long de la formation.
- Présentation de la structure et du format de l'examen.
- Conseils et astuces pour réussir l'examen.

CERTIFICATION

PECB Certified Lead Ethical Hacker

Cette formation prépare officiellement à l'examen PECB Certified Lead Ethical Hacker. Un code coupon vous sera fourni afin que vous puissiez programmer votre examen en ligne sur le site du PECB.

Modalités de l'examen PECB Lead Ethical Hacker

- **Type d'examen** : examen technique, compromettre 3 machines cibles et rédiger un rapport
- **Durée** : 06H00
- **Langues** : anglais, français et espagnol
- **Score requis** : 70 %
- **Livre ouvert** : autorisé (supports de cours et notes personnelles)
- **Surveillance** : en ligne via l'application PECB Exams

Après avoir réussi cet examen, vous pourrez demander la certification PECBCertified Lead Ethical Hacker.

À savoir : les certifications PECB sont valides 3 ans et doivent être maintenues en respectant les exigences de frais de maintenance annuels (AMF) et de crédits de développement professionnel continu (CPD). Pour en savoir plus sur les modalités, consultez le règlement d'examen PECB ainsi que le règlement de certification PECB.

MODALITÉS PÉDAGOGIQUES ET D'ÉVALUATION

- | | |
|---|--------------------------------------|
| ✓ Test de positionnement | ✓ Questionnaire d'évaluation à chaud |
| ✓ Supports pédagogiques remis aux participants | ✓ Feuilles d'émargement |
| ✓ Évaluation des acquis tout au long de la formation | ✓ Questionnaire d'évaluation à froid |
| ✓ Alternance d'apports théoriques et de travaux pratiques | ✓ Étude de cas |
| ✓ Examen officiel de certification | |

ACCESSIBILITÉ

Adaptations possibles pour les personnes en situation de handicap après analyse du besoin.