CLEH - Certified Lead Ethical Hacker : piratage éthique et tests d'intrusion

Date et durée

Code formation : CLEH
Durée : 4,5 jours
Nombre d'heures : 31 heures

Formation avec certification

PECB Certified Lead Ethical Hacker

Description

Aujourd'hui, avec la montée en flèche des **failles de sécurité** dans les PME et les grandes entreprises, on constate une forte demande en matière de hacking éthique. Cette discipline reste en effet une des meilleures armes pour sauvegarder les ressources et assurer la confidentialité des données et des personnes. De ce fait, maîtriser les **techniques de piratage éthique et de tests d'intrusion** constitue une nécessité pour tous ceux qui désirent se spécialiser dans la sécurité de l'information et la sécurité informatique.
Cette **formation de 4,5 jours** a pour objectif de vous doter des compétences et des connaissances indispensables pour mener des opérations avancées en hacking éthique. Vous serez plus précisément formé aux **techniques de test d'intrusion** sur des systèmes d'information et des infrastructures réseau. Le cours lead ethical hacker inclus **une série des labs sur une machine virtuelle** et des études de cas afin de vous permettre une mise en pratique rapide de la théorie.
À la fin de cette formation très utile et très demandée, vous serez prêt à passer l'examen officiel Lead Ethical Hacker. Cette examen en ligne vous permettra d'obtenir **le prestigieux titre de PECB Certified Lead Ethical Hacker** (*en savoir plus dans l'onglet certification*)**. CEH**
Télécharger le guide de formation PECB Lead Ethical Hacker

Objectifs

À l'issue de la formation lead ethical hacker, vous atteindrez les objectifs suivants :

- connaître parfaitement les concepts, les méthodes et les techniques employés par les acteurs de la cybersécurité et les hackers éthiques pour effectuer des tests d'intrusion ;
- comprendre les synergies existantes entre les méthodes de tests de pénétration, les normes et les réglementations ;
- développer une expertise approfondie en matière de hacking éthique et de ses usages ;
- réussir l'examen officiel et décrocher votre certification PECB Certified Lead Ethical Hacker.

Points forts

> Contrairement à la CEH, la formation CLEH met l'accent sur des travaux pratiques basés sur des cas réels et inclut une documentation complète de 450 pages.
> 35 crédits DPC sont attribués.
> L'examen de certification est inclus dans le prix de la formation.
> En cas d'échec à l'examen, vous pouvez le repasser sans frais dans un délai de 12 mois.

Certification

A la fin de la formation, vous recevrez un bon d'échange qui vous permettra de programmer votre examen de certification PECB Lead Ethical Hacker à la date et à l'heure de votre choix.

Informations sur l'examen Lead Ethical Hacker

L'examen est **en anglais et se déroule en ligne**. Il se compose d'une épreuve pratique et la rédaction d'un rapport pour lesquels vous disposez d'un maximum de 6 heures. Pour la partie pratique, vous devez **infecter au moins 2 machines cibles à l'aide d'un test de pénétration**. Pour la partie théorique, vous devrez rédiger vos opérations de piratage. Lors de cette épreuve, vous pourrez consulter les supports de cours et utiliser vos notes personnelles. **La note de passage est fixée à 70%**.
Une fois que vous avez réussi l'examen et satisfait aux exigences (*2 ans d'expérience en tests d'intrusion et cybersécurité*), vous pouvez **demander votre certification PECB Certified Lead Ethical Hacker.**

Pour en savoir plus sur les modalités, consultez le règlement d'examen PECB ainsi que le règlement de certification PECB.

Modalités d'évaluation

Travaux Pratiques
Etude de cas

Pré-requis

Suivre la formation lead ethical hacker nécessite les prérequis suivants :

- maîtriser les concepts et les principes applicables à la sécurité de l'information ;
- posséder des compétences avancées en administration de systèmes d'exploitation ;
- avoir de bonnes connaissances sur les réseaux et les techniques de programmation est fortement conseillé.

Public

Cette formation s'adresse aux publics suivants :

- les personnes désireuses de se familiariser avec les techniques de base utilisées pour mener à bien des tests d'intrusion ;
- les acteurs de la cybersécurité qui veulent maitriser les méthodes de piratage éthique et les techniques de tests d'intrusion ;
- les responsables SSI, notamment les cadres en charge de la sécurité de l'information et de la sécurité informatique en général ;
- les personnes impliquées en sécurité de l'information qui souhaitent approfondir leurs connaissances dans ce domaine ;
- les chefs de service ou les experts consultants désireux de savoir gérer des opérations de piratage éthique ;
- les administrateurs techniques qui souhaitent connaître comment planifier et exécuter un test de pénétration.

Cette formation s'adresse aux profils suivants

Administrateur système
Administrateur réseaux - télécoms
Architecte informatique / SI
Analyste cybersécurité
Pentester (tests d'intrusion)

Programme

Jour 1 : initiation au piratage éthique

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

Jour 2 : initiation de la phase de reconnaissance

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

Jour 3 : Initiation de 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.
- Les attaques côté client.
- Les attaques provenant des infrastructures Web.
- Les attaques par les réseaux sans fil (Wi-Fi).
- L'escalade des droits.
- Le pivoting réseau.
- Les transferts de fichiers.
- La conservation des accès.

Jour 4 et 5 : post-exploitation et rédaction de rapport

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

PECB

Training content delivered in partnership with PECB PECB