CLEH

Certified Lead Ethical Hacker

Certification PECB

Oo2 Formations & Consulting

PECB AUTHORIZED TITANIUM PARTNER

Hackers éthiques

votre meilleure défense en cybersécurité

Dans un contexte de cybermenaces croissantes, la protection des systèmes informatiques devient un enjeu critique pour toutes les organisations. La certification PECB Certified Lead Ethical Hacker (CLEH) prépare les professionnels à identifier et corriger les vulnérabilités des systèmes pour prévenir les cyberattaques. Ce programme de formation avancé combine expertise théorique et compétences pratiques pour répondre aux besoins de sécurité des entreprises.

Votre rôle : protéger, prévenir, performer

Dans un environnement numérique complexe et évolutif, le piratage éthique n'est plus une option, mais une nécessité. Avec CLEH, vous serez en mesure de :

- Évaluer vos systèmes comme un hacker professionnel : Identifiez les vulnérabilités avant qu'elles ne soient exploitées.
- Mettre en place des solutions robustes : Transformez les failles détectées en points forts.
- Rassurer vos partenaires et clients : Gagnez leur confiance grâce à une sécurité renforcée et prouvée.

Trois bonnes raisons de vous certifier CLEH

1. Maitrisez l'art du hacking éthique : Découvrez comment les hackers opèrent et anticipez leurs stratégies avec une méthodologie éprouvée.
2. Renforcez votre position sur le marché : Les certifications en cybersécurité sont parmi les plus recherchées par les employeurs. CLEH vous ouvre la porte à de nouvelles opportunités de carrière.
3. Protégez ce qui compte le plus : Les données sensibles, les infrastructures critiques et la réputation de votre organisation sont entre vos mains.

CLEH : une certification qui transforme les organisations...

pour les grandes entreprises

Renforcez la sécurité des systèmes d'information à chaque niveau, de l'architecture réseau aux applications critiques. Prévenez les fuites de données et les interruptions de service.

pour les PME et startups

Adoptez une stratégie de cybersécurité proactive à moindre coût. Faites de la certification CLEH un investissement stratégique pour sécuriser votre croissance.

pour les consultants en cybersécurité

Positionnez-vous en expert incontournable pour vos clients. CLEH vous offre une reconnaissance internationale et une méthodologie claire pour accompagner les organisations dans leur transformation numérique sécurisée.

Des résultats concrets grâce à CLEH

- Réduction des cyberattaques réussies : +80 % de protection supplémentaire en moyenne.
- Meilleure gouvernance de la sécurité IT : Des stratégies alignées sur les standards internationaux.
- Confiance renforcée des parties prenantes : Clients, partenaires et employés reconnaissent l'impact positif des initiatives CLEH.
- Optimisation des coûts : Un investissement dans CLEH permet à l'entreprise de réduire considérablement les dépenses liées aux attaques et à la récupération post-incidente.

Les **points forts** de la certification CLEH

1.

Approche complète et structurée : Vous apprenez à aborder la cybersécurité de manière proactive en identifiant les failles avant qu'elles ne soient exploitées.

2.

Méthodologies avancées : Formation basée sur des cadres internationaux comme le PTES (Penetration Testing Execution Standard) et l'OSSTMM (Open Source Security Testing Methodology Manual).

3.

Simulations réalistes : Des laboratoires interactifs permettent de reproduire des scénarios de cyberattaques en temps réel.

4.

Reconnaissance internationale : PECB est un leader mondial dans les certifications professionnelles, garantissant une reconnaissance de votre expertise.

Comparaison **entre le PECB CLEH et l'EC-Council CEH** : quelle certification choisir ?

Le hacking éthique est désormais une compétence cruciale. Parmi les certifications reconnues, le PECB Certified Lead Ethical Hacker (CLEH) et l'EC-Council Certified Ethical Hacker (CEH) offrent des approches différentes. Voici quelques-unes de ces différences clés :

Formation pratique et réaliste : Le PECB CLEH met l'accent sur des laboratoires interactifs et des études de cas réels, tandis que le CEH est davantage axé sur l'usage des outils techniques.

Alignement sur les normes mondiales : Le CLEH s'appuie sur des cadres internationaux (PTES, OSSTMM) pour former selon les meilleures pratiques, une approche moins marquée dans le CEH.

Équilibre technique et leadership : Le CLEH prépare non seulement à exécuter des tests, mais aussi à superviser des équipes et projets, offrant une perspective managériale idéale pour les décideurs.

Public cible : Le CEH est parfait pour les experts techniques ; le CLEH s'adresse également aux managers et stratèges cherchant à intégrer le hacking éthique dans leur vision globale.

Pour ceux qui veulent maîtriser les aspects techniques tout en développant des compétences en gestion et stratégie, le CLEH offre une valeur ajoutée unique.

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

avec certification

Code : CLEH Durée : 4,5 jours

Protégez vos systèmes avant qu'il ne soit trop tard. Devenez un hacker éthique certifié avec CLEH !

Objectif :

- 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.

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 : 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.

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

EN SAVOIR +

Examen de certification CLEH

L'examen comprend deux parties :

- Examen pratique : Les candidats doivent compromettre au moins deux machines cibles en réalisant des tests d'intrusion.
- Rédaction d'un rapport : Documentation détaillée du processus et des résultats des tests effectués.

- **Durée : 6 heures.**
- **Langue : L'examen est disponible en plusieurs langues, y compris le français.**
- **Note de passage : 70% de bonnes réponses.**

Certification CLEH : Pourquoi choisir Oo2 Formations ?

1.

Des formateurs certifiés et expérimentés : Bénéficiez de l'expertise de professionnels de terrain avec des années d'expérience en cybersécurité.

2.

Une approche personnalisée : Nos programmes s'adaptent aux besoins spécifiques de chaque entreprise, garantissant une meilleure pertinence des apprentissages.

3.

Support post-formation : Après la formation, bénéficiez d'un accompagnement pour mettre en œuvre les meilleures pratiques au sein de votre organisation.

4.

Réseau professionnel : Rejoignez une communauté mondiale de professionnels certifiés en cybersécurité.

5.

Les frais d'examen et de certification sont inclus dans le prix de la session de formation.


Oo2 Formations
& Consulting


PECB
AUTHORIZED
TITANIUM
PARTNER

Oo2 Formations & Consulting

PECB AUTHORIZED TITANIUM PARTNER

Contactez nous !

France

128, rue de la Boétie
75008 Paris

+33 (0)188 24 70 33
+33 (0)188 24 70 34

contact@oo2.fr