SAFETY FIRST CONSULTING
Notre expertise à votre service

PECB



PECB Certified
Lead Ethical Hacker

Développez vos connaissances en matière de piratage éthique et de sécurité informatique ; améliorez vos compétences en matière de piratage et perfectionnez votre connaissance des techniques les plus avancées en matière de sécurité informatique.

Pourquoi devriez-vous y participer ?

L'impact des incidents de sécurité dans les petites et grandes organisations a considérablement augmenté, tout comme la demande de piratage éthique. Le piratage éthique est l'un des outils les plus efficaces pour la sauvegarde des actifs et la protection des personnes et des informations. La certification en piratage éthique devient peu à peu une exigence standard pour les professionnels qui veulent travailler dans le domaine de la sécurité de l'information.

Une certification PECB Certified Lead Ethical Hacker vous aidera à démontrer votre capacité à évaluer légalement la sécurité des systèmes et à découvrir leurs vulnérabilités. Le cours offre des informations sur les dernières méthodes et outils de piratage éthique. Il fournit également une méthodologie pour effectuer des tests d'intrusion conformément aux normes et aux bonnes pratiques, telles que le Penetration Testing Execution Standard (PTES) et l'Open Source Security Testing Methodology (OSSTMM).

La compréhension des stratégies des pirates informatiques permet de résoudre les problèmes et les défis en matière de sécurité. Après avoir suivi cette formation, vous serez en mesure de planifier, de gérer et d'exécuter des tests d'intrusion de la sécurité des informations.

Le cours PECB Certified Lead Ethical Hacker repose sur le concept de la mise en pratique de ce que vous avez appris. Il comprend des sessions de laboratoire et des exemples pratiques pour vous aider à mettre la théorie en pratique.

La formation est suivie de l'examen de certification. Si vous réussissez, vous pourrez demander la certification « PECB Certified Lead Ethical Hacker ». Pour plus d'informations sur le processus d'examen, veuillez vous reporter à la section Examen, certification et informations générales ci-dessous.



À qui s'adresse la formation ?

Cette formation est destinée aux :

- Personnes souhaitant acquérir des connaissances sur les principales techniques utilisées pour réaliser des tests d'intrusion
- Personnes impliquées dans la sécurité de l'information qui cherchent à maîtriser les techniques de piratage éthique et de tests d'intrusion
- Personnes responsables des systèmes de la sécurité d'information, telles que les responsables de la sécurité de l'information et les professionnels de la cybersécurité
- Membres de l'équipe de sécurité de l'information voulant améliorer leurs connaissances de la sécurité de l'information
- Managers ou conseillers experts souhaitant apprendre à gérer des activités de piratage éthique
- Experts techniques souhaitant apprendre comment planifier et réaliser un test d'intrusion

Programme de la formation

Durée : 5 jours

Jour 1 | Introduction au piratage éthique

- Objectifs et structure de la formation
- Normes, méthodologies et cadres de tests d'intrusion
- Aperçu du laboratoire
- Concepts fondamentaux du piratage éthique
- Principes de base des réseaux
- Comprendre la cryptographie
- Tendances et technologies pertinentes
- Principes fondamentaux de Kali Linux
- Initiation du test d'intrusion
- Analyse de la portée du test d'intrusion
- Implications juridiques et accord contractuel

Jour 2 | Lancement de la phase de reconnaissance

- Reconnaissance passive
- Reconnaissance active
- Identification des vulnérabilités

Jour 3 | Lancement de la phase d'exploitation

- Modèle de menace et plan d'attaque
- Éviter les systèmes de détection d'intrusion
- Attaques côté serveur
- Attaques côté client
- Attaques des applications Web
- Attaques Wi-Fi
- Escalade des droits
- Pivotement
- Transferts des fichiers
- Conservation de l'accès

Jour 4 | Post-exploitation et rapports

- Nettoyage et destruction des artefacts
- Production d'un rapport des résultats
- Recommandations sur l'atténuation des vulnérabilités identifiées
- Clôture de la formation

Jour 5 | Examen de certification



Objectifs d’apprentissage

Cette formation vous permet de :

- Maîtriser les concepts, méthodes et techniques utilisés par les organisations de cybersécurité et les hackers éthiques pour réaliser des tests d’intrusion
- Reconnaître la corrélation entre les méthodologies de tests d'intrusion, les cadres réglementaires et les normes
- Acquérir une connaissance approfondie des composantes et des opérations du piratage éthique

Examen

Durée : 6 heures

L’examen « PECB Certified Lead Ethical Hacker » répond pleinement aux exigences du Programme d'examen et de certification (PEC) de PECB. L'examen couvre les domaines de compétence suivants :

Domain 1 | Outils et techniques de collecte d'informations

Domain 2 | Modélisation des menaces et identification des vulnérabilités

Domain 3 | Techniques d’exploitation

Domain 4 | Escalade des droits

Domain 5 | Pivotement et transferts de fichiers

Domain 6 | Rapports

L'examen PECB Certified Lead Ethical Hacker comprend deux parties : l'examen pratique et la rédaction du rapport. L'examen pratique exige du candidat qu'il compromette au moins deux machines cibles au moyen des tests d’intrusion. Le processus doit être documenté dans un rapport écrit. L'examen PECB Certified Lead Ethical Hacker est un examen à livre ouvert. Les candidats sont autorisés à utiliser les supports de cours et leurs notes personnelles pendant l'examen.

Pour des informations spécifiques sur le type d'examen, les langues disponibles et d'autres détails, veuillez consulter la liste des examens PECB et les Politiques et règlements relatifs à l’examen.



Certification

Après avoir réussi l'examen, vous pouvez demander la certification « PECB Certified Lead Ethical Hacker », en fonction de votre niveau d'expérience, comme indiqué dans le tableau ci-dessous. Vous recevrez le certificat une fois que vous aurez satisfait à toutes les exigences éducatives et professionnelles pertinentes.

Titre de compétence	Examen	Expérience professionnelle	Expérience de projet	Autres exigences
PECB Certified Lead Ethical Hacker	Examen PECB Certified Lead Ethical Hacker	**Deux années d'expérience en matière de tests d'intrusion et de cybersécurité**	Aucune	Signature du Code de déontologie de PECB et du Code de conduite pour les PECB CLEH

Pour plus d'informations sur les certifications en piratage éthique et le processus de certification PECB, veuillez vous référer aux Politiques et règlements relatifs à certification.

Informations générales

- Les participants recevront le support de formation contenant plus de 450 pages d'informations, d'exemples pratiques et d'exercices.
- Une Attestation d'achèvement de formation de 35 unités de FPC (Formation professionnelle continue) sera délivrée aux participants ayant suivi la formation.
- Les candidats qui ont suivi le cours mais n'ont pas réussi l'examen peuvent le reprendre une fois gratuitement dans les 12 mois à compter de la date initiale de l'examen.