

Formation Lead Ethical Hacker + Certification

Présentation

En partenariat avec PECB, cette formation permet aux participants de développer les compétences et les connaissances nécessaires pour effectuer du piratage éthique, principalement pour les tests d'intrusion des systèmes d'information et des réseaux.

Outre des informations théoriques, le cours comprend également des laboratoires qui sont réalisés avec une machine virtuelle.

Durée : 35,00 heures (5 jours)

Tarif INTRA : Nous consulter

Objectifs de la formation

- 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

Prérequis

Avoir une connaissance des concepts et principes de sécurité de l'information et des compétences avancées en matière de systèmes d'exploitation, des réseaux informatiques et des concepts de programmation.

Public

- 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

J1 : Introduction au piratage éthique

- 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

J2 : Lancement de la phase de reconnaissance

- Reconnaissance passive
- Reconnaissance active
- Identification des vulnérabilités

J3 : 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

J4 : 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

J5 : Préparer l'examen

Cette formation vous prépare à l'examen de certification de PECB. (Certification incluse)

- Langue : Français
- Durée : 6 heures
- Format : Examen en ligne

L'examen couvre les domaines de compétences suivants :

- **Domaine 1** : Outils et techniques de collecte d'informations
- **Domaine 2** : Modélisation des menaces et identification des vulnérabilités
- **Domaine 3** : Techniques d'exploitation
- **Domaine 4** : Escalade des droits
- **Domaine 5** : Pivotement et transferts de fichiers
- **Domaine 6** : Rapports

Pour de plus amples informations concernant l'examen, veuillez consulter [Politiques et règlement d'examen.](#)

En cas d'échec, les candidats ont l'opportunité de présenter à nouveau l'examen dans un délai de 12 mois après leur première tentative.

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation *(évaluations en ligne dans l'extranet apprenant)*

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.