

## 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**

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

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

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Évaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

## **Accessibilité**

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