Devenir Lead Ethical Hacker

Acquérir une compréhension approfondie des concepts et méthodes employés par les professionnels de la cybersécurité en vue d'exécuter des tests d'intrusion.

Ref: PR-CYB-AT-LEH

DURÉE : **5 Jours** (35H)
Prix : **3 590,00 € HT**

PRÉSENTIEL

Objectifs et compétences visés

- 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 de piratage éthique.

À qui s'adresse la formation ?

Profils

- 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 souhaitent maîtriser les techniques de piratage éthique et de tests d'intrusion.
- Responsables de la sécurité des systèmes d'information et membres d'une équipe de sécurité de l'information cherchant à améliorer leurs connaissances en matière de sécurité de l'information.
- Managers ou experts souhaitant apprendre à gérer les activités de piratage éthique.

Prérequis

Aucun prérequis n'est nécessaire à cette formation. Il est nécessaire de venir muni d'un ordinateur portable.

Contenu de la formation

Introduction au piratage éthique

- Normes, méthodologies et cadres des tests de pénétration
- Concepts fondamentaux du piratage éthique et de la cryptographie et principes de base des réseaux
- Tendances et technologies pertinentes
- Principes de base de Kali Linux
- Initiation aux tests d'intrusion et analyse de leur portée
- Implications juridiques et accord contractuel

Initiation et début de la phase de reconnaissance

- Reconnaissance passive et active
- Identification des vulnérabilités
- Modèle de menace et plan d'attaque
- Contournement des systèmes de détection d'intrusion
- Attaques : côté serveur, côté client, des applications web et attaques WIFI
- Escalade de privilèges et pivotage
- Transferts de fichiers et maintien de l'accès

Actions post-exploitation et rapport

- Nettoyage et destruction des artefacts
- Génération d'un rapport
- Recommandations sur l'atténuation des vulnérabilités identifiées

Modalités

Modalités d'évaluation

Cette formation se conclut par un examen de certification PECB.

Nos plus

Cette formation est animée par un consultant CNPP certifié Lead Ethical Hacker et expert en audits techniques.
Disponible en visioconférence.

En bref

21000
stagiaires / an

Des infrastructures pédagogiques uniques

+ de 500
diplômés / an

+ de 400
intervenants

Les prochaines sessions

Du 09/09/24 au 13/09/24 **Paris** **3 590,00 € HT**

Du 04/11/24 au 08/11/24 Paris 3 590,00 € HT

Nos formations complémentaires

Cybersécurité~Forensic et sécurité opérationnelle
Fondamentaux techniques de la sécurité de l'information
1 Jour
Présentiel
Découvrez les fondamentaux techniques de la sécurité de l'information (sécurité opérationnelle)

Cybersécurité~Forensic et sécurité opérationnelle
Devenir Lead Operational Security Officer (SECOPS)
5 Jours
Présentiel
Maîtriser les principes et mécanismes techniques de la sécurité de l'information sur le plan opérationnel

Besoin d'informations sur une formation en cybersécurité ?

Nous sommes à votre écoute pour échanger sur votre prochaine formation en cybersécurité.

Contactez-nous !

(+33)1 75 43 51 01