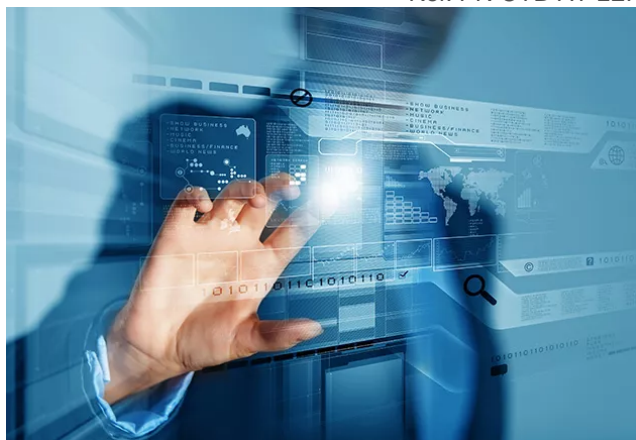


Acquérir une compréhension approfondie des concepts et méthodes employés par les professionnels de la cybersécurité en vue d'exécuter des tests d'intrusion.



DURÉE : 5,5 Jours (37H30)

Prix : 3 665,00 € 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 - première partie

- Normes, méthodologies et cadres des tests d'intrusion
- Présentation du lab
- Concepts fondamentaux du piratage éthique
- Principes de base des réseaux
- Fondamentaux de la cryptographie

Introduction au piratage éthique - seconde partie

- Fondamentaux de la cryptographie
- Tendances et technologies pertinentes
- Principes de base de Kali Linux
- Initiation du test d'intrusion
- Analyse de la portée du test d'intrusion
- Implications juridiques et accord contractuel

Phase de reconnaissance - première partie

- Reconnaissance passive
- Reconnaissance active

Phase de reconnaissance - seconde partie

- Identification des vulnérabilités

Phase d'exploitation - première partie

- Modèle de menace et plan d'attaque
- Contournement des systèmes de détection d'intrusion
- Attaques côté serveur
- Attaques côté client
- Attaques des applications web

Phase d'exploitation - seconde partie

- Attaques WIFI
- Escalade de privilèges
- Pivotage
- Transferts de fichiers
- Maintien de l'accès

Post-exploitation et rapport - première partie

- Nettoyage et destruction des artefacts
- Génération d'un rapport

Post-exploitation et rapport - seconde partie

- Recommandations sur l'atténuation des vulnérabilités identifiées

Matinée de révisions

- Sujets libres
- Préparation à l'examen

Examen de certification PECB

- 6 heures d'examen pratique sur le lab PECB, sur un des créneaux d'examen disponibles
- Rédaction et soumission du rapport dans les 24h qui suivent

Modalités de la formation

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.

CNPP en quelques chiffres

21000

stagiaires / an



Des infrastructures
pédagogiques uniques

+ de 500

diplômés / an

+ de 400

intervenants

98%

de stagiaires satisfaits en
2025

Nos formations complémentaires

Forensic et sécurité opérationnelle

Formation cybersécurité : Fondamentaux techniques de la sécurité de l'information

1 Jour

Présentiel

Appréhender les différentes facettes de la sécurité technique (authentification, développement, SI central...)

-

Forensic et sécurité opérationnelle

Formation cybersécurité : Devenir Lead Ethical Hacker

5,5 Jours

Présentiel

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

-

Besoin d'informations sur une formation en cybersécurité ?

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

Contactez-nous !

+33 (0)8 06 00 03 80