Hacking éthique : Concepts avancés

DOMAINE : *Hacking étique*
CATEGORIE : *Offensive*

MISE A JOUR LE 13/01/2025

Descriptif

De nos jours, la sécurité informatique est devenue un enjeu de taille pour les **entreprises**. En effet, ces deux dernières années, **70% des cyberattaques** ont visé des **sociétés** pouvant causer des désagréments allant du vol de données jusqu'à la mise en danger des vies humaines. Il est indispensable que le tissu **industriel** se protège contre les **cybermenaces**.

Cette formation **avancée** en **hacking éthique** est conçue pour les professionnels de la sécurité souhaitant **approfondir** leurs compétences et leurs connaissances.

Elle met en avant les techniques et les outils avancés pour identifier, **exploiter** et répondre aux vulnérabilités des systèmes digitaux de manière éthique et légale.

En plus de savoir sécuriser les systèmes informatiques contre les attaques **sophistiquées**, les participants seront capables d'**évaluer** la maturité d'une organisation en matière de **sécurité** informatique.

Informations

Référence	**CY-HE-HECA**

Publics concernés

Professionnel de la sécurité souhaitant approfondir ses connaissances.

Formateur

Expert certifié en cybersécurité

Prérequis

Avoir les connaissances de bases en hacking éthique.

Certification préparée

Aucune

Objectifs

- Comprendre et identifier les **principales menaces**.
- Savoir analyser et **collecter** des données sur un **réseau**.
- Savoir identifier les **vulnérabilités** et les **exploiter**.
- Savoir développer une **stratégie de défense**.
- Être initié aux **audits de sécurité**.

Type de session

Intra-entreprise, **inter-entreprise** (en présentiel ou à distance)

Durée	4 jours (28 heures)
Date	À la demande
Tarif	2.450 € H.T
Effectif	12 participants max
Niveau	**Intermédiaire**
Délai d'accès	**3 semaines**

Programme

1) Rappel sur le hacking éthique

- Reconnaître les principaux acteurs et leurs rôles associés
- La confidentialité, l'intégrité et la disponibilité
- Cadre légal et éthique

2) Analyse des réseaux

- Scan et énumération
- Identifier les vulnérabilités d'un réseau
- Analyser le trafic réseau et collecter les données
- Contourner un sniffer réseau
- Les principales attaques et contre-mesures

3) Mise en œuvre d'un hacking éthique

- Les mots de passe, haches et attaques associées
- Comprendre le fonctionnement des logiciels espions
- Mise en œuvre d'une escalade de privilèges
- Les rootkits, fonctionnement et mise en œuvre
- Comprendre les attaques par stéganalyse
- Savoir effacer ses traces

4) Ingénierie sociale et malware

- Techniques d'ingénierie sociale
- Les virus et les vers
- Techniques de contre-mesures

5) Les attaques sur services et sessions

- Le Denial of Service (DoS)
- Le détournement de session
- Les attaques basées sur les réseaux sans fil
- Prévention et contre-mesures

6) Les attaques orientées web

- Fonctionnement des serveurs web
- Principales vulnérabilités des applications web
- Attaques des applications web et contre-mesures

7) Les attaques orientées applications

- L'injection de SQL, techniques d'évasion et contre-mesures
- Méthodes de détection des buffers overflows

8) Les attaques sur plateformes mobiles

- Les attaques sur mobiles (Android et iOS)
- Les attaques sur IoT et OT
- Techniques de contre-mesures

9) Les autres types d'attaques

- Les attaques orientées Cloud Computing
- Les attaques sur cibles physiques
- Bypasser la sécurité d'un réseau
- Techniques d'évasion (IDS, Firewall et Honeypot)

10) Les Pentests et audits de sécurité

- Méthodologies liées aux tests d'intrusion
- Initiation aux audits de sécurité

11) Mise en situation réelle

- Étude de cas réel au sein d'un laboratoire virtuel

Ce programme peut être adapté pour des sessions plus courtes, plus longues ou selon des besoins spécifiques

Modalités pédagogiques

Nous mettons en œuvre des modalités pédagogiques **variées** afin de maintenir l'attention des participants. Cette formation s'appuiera sur :

- Une alternance théorie (35%) et pratique (65%).
- Des mises en situation réelle, études de cas et échanges de pratiques.
- Des mises à disposition d'outils numériques interactifs, collaboratifs et participatifs.

À la fin de la formation, toutes les ressources pédagogiques seront **mises à disposition** pour tous les participants via leur espace dédié.

Modalités d'évaluation et de suivi

Les acquis de l'action de formation sont **évalués** à partir des productions des participants lors des études de cas et à partir de quiz et exercices réguliers.

Un questionnaire **d'autoévaluation** au regard des objectifs de la formation vous sera transmis avant le début de la formation et à la fin de celle-ci, vous permettant ainsi de mesurer votre progression en fin de formation.

Information sur l'accessibilité

Nous remercions les personnes qui auraient des **besoins spécifiques** de nous le signaler dès leur inscription. Quel que soit le type de handicap, nous pouvons adapter certaines de nos modalités de formation en étudiant ensemble vos besoins. Pour toutes questions, merci de contacter notre **référent handicap** :

- Par mail à handicap@ghdeformation.fr
- Ou par téléphone au +33 06 78 84 71 24