Certified Ethical Hacker Master (CEHM)

Description

Renforcez vos compétences avec la certification Certified Ethical Hacker Master (CEHM)

La certification Certified Ethical Hacker Master (CEHM) s'adresse aux experts en sécurité informatique ayant déjà obtenu la prestigieuse certification CEH V12. Cette formation avancée permet d'approfondir vos compétences en piratage éthique à travers des scénarios d'attaque réels. Vous aurez accès à plus de 100 labs pour perfectionner vos techniques de défense et d'attaque en cybersécurité. Ce cours vous prépare également au passage de l'examen CEH Master, un test exigeant qui mettra à l'épreuve votre capacité à identifier des vulnérabilités et à sécuriser des systèmes. La formation CEHM est conçue pour les professionnels souhaitant se distinguer dans le domaine de la cybersécurité.

Une certification pour les experts en sécurité informatique

En suivant cette formation, vous maîtriserez des outils et techniques avancés pour mener des tests de pénétration, analyser des failles de sécurité et sécuriser les réseaux. Grâce à une approche pratique et un accès à des outils de pointe, vous serez prêt à affronter les défis actuels de la sécurité des systèmes d'information.

Niveau
Avancé
Contenu du cours
Module 1 : Introduction au piratage éthique

- Les éléments de la sécurité de l'information
- La méthode Cyber Kill Chain
- La base de connaissances MITRE ATT&CK®
- Les types de hackers
- Le hacking éthique
- L'assurance de l'information (IA)
- La gestion des risques
- La gestion des incidents
- Les réglementations PCI DSS, HIPPA, SOX et RGPD

Module 2 : Empreinte et reconnaissance

- Réaliser une analyse d'empreinte du réseau cible à l'aide de moteurs de recherche, de services web et de sites de réseaux sociaux
- Réaliser des empreintes de sites web, de courriels, de whois, de DNS et de réseaux sur le réseau cible

Module 3 : Analyse des réseaux

- Détecter les hôtes, les ports, les services et les systèmes d'exploitation sur le réseau cible
- Réaliser des analyses sur le réseau cible au-delà des IDS et des pare-feux

Module 4 : Phase d'énumération

- Réaliser une énumération NetBIOS, SNMP, LDAP, NFS, DNS, SMTP, RPC, SMB et FTP

Module 5 : Analyse de vulnérabilité

- Réaliser une recherche de vulnérabilité à l'aide de systèmes d'évaluation de la vulnérabilité et de bases de données
- Réaliser une évaluation de la vulnérabilité à l'aide de divers outils d'évaluation de vulnérabilité

Module 6 : Piratage du système

- Exécuter une attaque dynamique en ligne afin de découvrir le mot de passe d'un système
- Effectuer une attaque par débordement de mémoire tampon afin d'accéder à un système distant
- Augmenter les niveaux de permissions en utilisant des outils d'escalade des niveaux de privilèges
- Augmenter les droits d'accès sur une machine Linux
- Masquer des données à l'aide de la stéganographie
- Supprimer des logs Windows et Linux en utilisant différents outils
- Cacher des artefacts sous Windows et Linux

Module 7 : Menaces de logiciels malveillants

- Prendre le contrôle d'une machine victime à l'aide d'un cheval de Troie
- Infecter un système cible en utilisant un virus
- Effectuer une analyse statique et dynamique de logiciels malveillants

Module 8 : Attaques par sniffing

- Exécuter des attaques de type MAC Flooding, ARP Poisoning, MITM et DHCP Starvation
- Usurper l'adresse MAC d'une machine Linux
- Réaliser un sniffing de réseau à l'aide de différents outils
- Détecter les attaques par empoisonnement dans un réseau à base de switchs

Module 9 : Ingénierie sociale

- Procéder à une ingénierie sociale en utilisant plusieurs techniques
- Usurper l'adresse MAC d'une machine Linux
- Détecter une attaque par hameçonnage
- Auditer la sécurité d'une entreprise pour détecter des attaques d'hameçonnage

Module 10 : Attaques par déni de service (DDoS)

- Effectuer une attaque DoS et DDoS sur un hôte cible
- Détecter des attaques DoS et DDoS et y répondre

Module 11 : Détournement de session

- Réaliser un détournement de session en utilisant plusieurs outils
- Détecter un détournement de session

Module 12 : Contournement des IDS, des pare-feu et des honeypots

- Contourner un pare-feu Windows
- Contourner des règles de pare-feu en utilisant des tunnels
- Contourner un antivirus

Module 13 : Piratage de serveurs Web

- Effectuer une reconnaissance sur un serveur Web en utilisant plusieurs outils
- Énumérer des informations concernant un serveur Web
- Déchiffrer des identifiants FTP en utilisant la méthode de l'attaque par dictionnaire

Module 14 : Piratage d'applications Web

- Réaliser une reconnaissance d'application Web en utilisant plusieurs outils
- Créer une araignée Web
- Effectuer un balayage de vulnérabilité d'une application Web
- Effectuer une attaque brute
- Effectuer une attaque de type Cross-site Request Forgery (CSRF)
- Identifier des failles XSS dans des applications Web
- Détecter des failles dans des applications Web en utilisant plusieurs outils de sécurité

Module 15 : Injections SQL

- Réaliser une attaque par injection SQL contre MSSQL afin d'extraire des bases de données
- Détecter des failles d'injection SQL en utilisant plusieurs outils

Module 16 : Piratage des réseaux sans fil

- Tracer l'empreinte d'un réseau sans fil
- Effectuer une analyse des communications sans fil
- Pirater un réseau WEP, WPA et WPA2
- Créer un point d'accès pirate pour capturer des paquets de données

Module 17 : Piratage des appareils mobiles

- Hacker un appareil Android via la création de charges utiles binaires
- Exploiter la plateforme Android via ADB
- Pirater un appareil Android via la création d'un fichier APK
- Sécuriser des appareils Android en utilisant plusieurs outils de sécurité Android

Module 18 : Piratage IoT et OT

- Collecter des informations via des outils d'empreinte en ligne
- Capturer et analyser des flux de données sur des appareils IoT

Module 19 : Cloud computing

- Réaliser une énumération des buckets S3 en utilisant plusieurs outils
- Exploiter des buckets S3 ouverts
- Augmenter les droits d'un utilisateur IAM en exploitant la politique utilisateur mal définie

Module 20 : Cryptographie

- Calculer les hachages MD5
- Réaliser un chiffrement de fichier et de message texte
- Créer et utiliser des certificats auto-signés
- Réaliser un cryptage de courrier électronique et de disque
- Réaliser une analyse cryptographique en utilisant plusieurs outils

Documentation

- Support de cours numérique inclus

Examen

- Ce cours prépare à la certification Certified Ethical Hacker (Practical).
- Pour obtenir la certification Certified Ethical Hacker (Practical), les candidats doivent réussir l'examen : 312-50 (ECC EXAM).
- Nombre de questions : 125
- Durée : 4 heures
- Si vous souhaitez passer cet examen, veuillez contacter notre secrétariat qui vous informera du coût des examens et prendra en charge toutes les démarches administratives nécessaires pour vous.

Profils des participants

- Analystes en cybersécurité
- Auditeurs internes et externes
- Administrateurs systèmes et réseaux
- Ingénieurs réseaux et systèmes
- Consultants en sécurité informatique

Connaissances Préalables

- Avoir une solide connaissance des concepts de cybersécurité
- Comprendre les bases du piratage éthique (CEH V12 requis)
- Maîtriser les techniques de scan de réseau et d'analyse de vulnérabilité
- Savoir manipuler des outils de test de pénétration
- Connaître les protocoles réseaux (TCP/IP, DNS, HTTP)

Objectifs

- Maîtriser les techniques avancées de piratage éthique
- Identifier et exploiter des vulnérabilités dans des systèmes cibles
- Procéder à des attaques de type DDoS et analyse des malwares
- Réaliser des tests de pénétration sur des réseaux sans fil et mobiles

- Sécuriser des serveurs Web et des applications Web
- Exploiter les failles de sécurité dans des environnements cloud
- Réussir l'examen CEH Master et obtenir la certification

Description
Formation Certified Ethical Hacker Master (CEHM)
Prix de l'inscription en Présentiel (CHF)
5900
Prix de l'inscription en Virtuel (CHF)
5650
Durée (Nombre de Jours)
5
Reference
CEHM