Organisme de formation professionnelle continue
Numero agrément 91 30 03332 30
France : +33 (0)188 24 70 33 / 34
Site : www.oo2.fr
Mail : contact@oo2.fr

Devenir maître certifié en piratage éthique (CEH Master)

Date et durée

Code formation : CEHM-FR
Durée : 5 jours
Nombre d'heures : 35 heures

Formation avec certification

C|EH Master : Certified Ethical Hacking Master

Description

La certification CEH Master est destinée aux professionnels de la sécurité informatique qui souhaitent approfondir leurs compétences en matière de piratage éthique et qui on **déjà obtenue la prestigieuse certification CEH V12**. De ce fait, en suivant cette formation vous serez préparer pour le passage de l'examen CEH Master compris dans notre offre.
Les **20 modules de cours CEH Master** que nous vous proposons vous permettront de renforcer vos compétences et de mettre en pratique tout ce que vous avez appris dans la formation CEH V12. En effet, grâce à plus de 100 labs, vous pourrez **observer des scénarios d'attaque en temps réel**, afin de réagir comme si vous étiez sur le terrain. De plus, vous aurez accès à un grand nombre d'outils qui vous permettront de **maitriser les techniques avancée du piratage éthique**.
A la fin de cette formation de 5 jours, vous pourrez vous présenter à **l'examen C|EH Practical** disponible en ligne. Cet examen exigeant dure 6 heures et vous devez démontrer que vous maîtrisez l'identification des vecteurs de menace, l'analyse des réseaux, la détection des systèmes d'exploitation, l'analyse des vulnérabilités, le piratage des systèmes, etc.

Objectifs

Après avoir suivi la **formation CEH Master**, vous validerez les objectifs suivants :

- comprendre le fonctionnement des vecteurs d'attaque ;
- procéder à un balayage réseau afin d'identifier les machines actives et vulnérables dans un réseau ;
- procéder à une récupération de bannières de systèmes d'exploitation et lister les services et les utilisateurs ;
- réaliser un piratage de système, une stéganographie, une attaque par stéganalyse et une dissimulation de traces ;
- identifier et exploiter des virus, des vers informatiques et des malwares afin de tirer profit de systèmes ;
- procéder à un sniffing (reniflage de paquets) ;
- effectuer une série d'attaques sur des serveurs et des applications web, incluant une exploration des répertoires, une altération des paramètres, un Cross-site Scripting, etc. ;
- effectuer des attaques par injection SQL ;
- effectuer tous types d'attaques par cryptographie ;
- réaliser des analyses de vulnérabilité en vue d'identifier des failles de sécurité ;
- réussir l'examen CEH Pratical et obtenir la certification Master C|EH®.

Oo2 est accrédité par EC-Council pour dispenser la formation CEH Master. Ce statut garantit la prestation d'un formateur agréé, des supports de cours officiels et des examens de certifications organisés en fin de formation.

Points forts

Une formation 100% pratique dirigée par un formateur expert en sécurité et accrédité par le EC-Council, + de 100 labs simulant des scénarios d'attaque en temps réel et un accès à une large gamme d'outils de piratage éthique.

Certification

En suivant notre formation CEH Master, vous pourrez **passer à tout moment l'examen CEH Pratical** de notre partenaire certificateur EC-Council. Cet examen, disponible en ligne et en anglais, consiste à **relever 20 défis pratiques** pendant une durée maximum de 6 heures. Pour décrocher le certification de Certified Ethical Hacker Master, vous devez **obtenir 70 % de bonnes réponses**.
Cette titre professionnel démontre ainsi que vous possédez des **compétences avancées en matière de piratage éthique et de sécurité informatique**, ce qui est important dans un contexte où la protection des systèmes informatiques est cruciale pour de nombreuses entreprises.

> **A noter :** *la certification professionnelle CEH Master est soumise à un processus de renouvellement et de maintien du niveau de compétence. Les exigences sont publiées sur la politique de formation continue de l'EC-Council (ECE).*

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre la **formation CEH Master** nécessite le prérequis suivant :

- Avoir suivi la formation de hacker éthique certifié et réussir l`examen CEH V12.

Public

Cette formation s'adresse aux publics suivants :

- les responsables sécurité des systèmes d'information, les auditeurs, les administrateurs de sites, les professionnels de la cybersécurité ainsi que tous autres personnes qui souhaitent sécuriser leurs infrastructures informatiques.

Cette formation s'adresse aux profils suivants

Analyste cybersécurité
Auditeur interne / externe
Administrateur réseaux - télécoms
Administrateur système
Ingénieur réseaux - télécoms
Ingénieur système

Programme

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 : l'empreinte et la 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 : l'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 : la phase d'énumération

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

Module 5 : l'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 : le 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 : les 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 : les 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 : l'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 : les 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 : le détournement de session

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

Module 12 : le 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 : le 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 : le 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 : les 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 : le 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 : le 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 : le 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 : le 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 : la 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.

CEH® est une marque déposée de EC-Council aux États-Unis.