SANCFIS

TRAINING CENTER

Certified Ethical Hacking

- **Référence :** CEH v12
- **Durée :** 5 jours

C | EH Certified Ethical Hacking

RESUME

Le CEH (Certified Ethical Hacker) est un professionnel de haut niveau spécialisé en sécurité informatique. Contrairement aux « black hats », qui sont des criminels informatiques, les hackers éthiques sont respectueux des lois et de la morale. Ils sont capables d'identifier les faiblesses et les vulnérabilités des systèmes et des réseaux, mais ne les exploitent que pour permettre aux entreprises ou aux organisations de mieux sécuriser leurs actifs informatiques et de mieux se protéger contre les cyberattaques.

En suivant cette formation CEH v12, vous développerez de solides compétences et bénéficierez de toute l'expérience pratique du piratage éthique. Vous apprendrez à utiliser les derniers outils, techniques et méthodes de hacking modernes dont se servent les hackers et les spécialistes de la sécurité de l'information pour attaquer une organisation en toute légalité.

À travers 20 modules qui vous aident à maitriser les bases du piratage éthique, vous serez également préparé pour passer le nouvel examen de certification CEH V12 (plus d'infos dans l'onglet certification). En effet, cette formation CEH évolue et prend en compte les nouvelles améliorations apportées par notre partenaire certificateur EC-Council.

Les nouveautés du Certified Ethical Hacker v12

Le programme C|EH® v12 a été repensé pour vous permettre d'apprendre tous les éléments indispensables à la pratique du piratage éthique moderne. Il comprend des nouveaux cours, des nouveaux labs, de nouvelles évaluations, des simulations d'engagement ainsi qu'une série de compétitions mondiales de piratage informatique.

Le CEH v12 repose également sur un nouveau modèle d'apprentissage fondé sur une approche méthodologique divisée en 4 phases : apprendre, se certifier, s'engager et se mesurer.

PARTICIPANTS

tout professionnel informatique débutant ou expérimenté dans le domaine de la cybersécurité.

Vous êtes responsable de la sécurité des systèmes d'information, administrateur réseaux, responsable informatique ou décisionnaire et êtes concerné par l'intégrité de l'infrastructure réseau ?

Cette formation s'adresse aux profils suivants

Administrateur système

Ingénieur système

Analyste cybersécurité

Technicien Support / HelpDesk

Auditeur interne / externe

Prérequis

Avoir 2 ans d'expérience minimum dans le domaine de la sécurité informatique.

OBJECTIFS

A l'issue de la formation CEH, vous atteindrez les objectifs suivants :

- ✓ Développer des compétences spécifiques en système et réseau informatique ;
- ✓ Connaitre et maîtriser les outils de hacking ;
- ✓ Maîtriser les méthodologies de piratage et d'intrusion éthique ;
- ✓ Comprendre les lois et l'éthique forte à respecter pour toute personne certifiée CEH ;
- ✓ Connaitre et savoir réaliser un audit de sécurité ;
- ✓ Réussir l'examen et obtenir la certification C|EH® v12 du EC-Council.

CONTENU

Module 1 : introduction au piratage éthique :

Ce module aborde les aspects clés du monde de la sécurité de l'information, tels que les principes de base du piratage éthique, les contrôles de sécurité de l'information, les lois en vigueur et les procédures standard.

Vous aborderez la méthodologie Cyber Kill Chain, le cadre MITRE ATT&CK, les classes de hackers, qu'est-ce que le piratage éthique, l'assurance de l'information (IA), la gestion des risques et des incidents, les normes de sécurité (PCI DSS, HIPPA, SOX) ainsi que le règlement générale sur la protection des données (RGPD).

Module 2 : l'empreinte et la reconnaissance

Ce module vous apprend à mettre en œuvre les techniques et les outils les plus récents pour réaliser des empreintes digitales et une reconnaissance. 30 exercices pratiques sont proposés.

Module 3 : l'analyse des réseaux

Ce module couvre les aspects fondamentaux des problèmes de sécurité de l'information au niveau des réseaux, notamment les règles de base du piratage éthique, les contrôles de sécurité de l'information, les lois pertinentes et les procédures standard. 10 exercices pratiques avec des cibles simulées réelles sont proposés.

Module 4 : la phase d'énumération

Ce module vous présente des techniques d'énumération variées, telles que les exploits BGP (Border Gateway Protocol) et NFS (Network File Sharing), ainsi que les contre-mesures associées. 20 exercices pratiques avec des cibles simulées réelles sont proposés.

Module 5 : l'analyse de vulnérabilité

Ce module vous apprend à identifier les failles de sécurité dans les réseaux, dans les infrastructures de communication et dans les terminaux d'une organisation cible. 5 exercices pratiques avec des cibles simulées réelles sont proposés.

Module 6 : le piratage du système

Ce module décrit différentes méthodes de piratage de systèmes, notamment la stéganographie, les attaques par stéganalyses et les chemins de fuite qui sont utilisés pour détecter les vulnérabilités des systèmes et des réseaux. 25 exercices pratiques avec des cibles simulées réelles sont proposés.

Module 7 : les menaces de logiciels malveillants

Ce module présente les types de logiciels malveillants, notamment le cheval de Troie, le virus et le ver, ainsi que l'audit du système pour les attaques de malware, l'analyse des logiciels malveillants et les solutions de prévention. 20 exercices pratiques avec des cibles simulées réelles sont proposés.

Module 8 : les attaques par sniffing

Dans ce module de ceh12, vous apprendrez les techniques de sniffing de paquets et comment les exploiter pour découvrir les vulnérabilités du réseau, ainsi que les

techniques de défense face aux attaques de sniffing. 10 exercices pratiques avec des cibles simulées réelles sont proposés.

Module 9 : l'ingénierie sociale

Ce module traite des concepts et des techniques d'ingénierie sociale, et notamment comment identifier les tentatives de vol, analyser les vulnérabilités sur le plan humain et proposer des solutions de lutte contre l'ingénierie sociale. 4 exercices pratiques avec des cibles simulées réelles sont proposés.

Module 10 : les attaques par déni de service (DDoS)

Ce module vous présente les diverses techniques d'attaque par déni de service (DoS) et par déni de service distribué (DDoS), ainsi que les outils nécessaires pour auditer une cible et concevoir des mesures de protection et de lutte contre les DoS et DDoS. 5 exercices pratiques avec des cibles simulées réelles sont proposés.

Module 11 : le détournement de session

Ce module vous aide à comprendre les diverses techniques de détournement de session (Hijacking) servant à détecter les faiblesses dans la gestion des sessions, l'authentification, l'autorisation et la cryptographie au niveau du réseau, et à définir des solutions pour y remédier. 4 exercices pratiques avec des cibles simulées réelles sont proposés.

Module 12 : le contournement des IDS, des pare-feu et des honeypot

Ce module vous initie au fonctionnement des pare-feu, des systèmes de détection d'intrusion et des honeypots, ainsi qu'aux outils utilisés pour détecter les faiblesses du périmètre d'un réseau et mettre en place des solutions de prévention. 8 exercices pratiques avec des cibles simulées réelles sont proposés.

Module 13 : le piratage de serveurs Web

Ce module vous fait comprendre les attaques de serveurs Web, incluant notamment une méthode d'attaque complète permettant d'auditer les vulnérabilités de l'infrastructure des serveurs Web et les solutions à appliquer. 7 exercices pratiques avec des cibles simulées réelles sont proposés.

Module 14 : le piratage d'applications Web

Ce module vous fait comprendre les attaques d'applications Web, incluant notamment une méthode d'attaque complète permettant d'auditer les vulnérabilités de l'infrastructure des apps et les solutions à appliquer. 15 exercices pratiques avec des cibles simulées réelles sont proposés.

Module 15 : les injections SQL

Ce module vous présente les techniques d'attaque par injection SQL, les outils de détection d'injection et les solutions pour détecter et se défendre contre les attaques par injection SQL. 4 exercices pratiques avec des cibles simulées réelles sont proposés.

Module 16 : le piratage des réseaux sans fil

Ce module vous présente le fonctionnement du cryptage sans fil, les méthodes et les outils de piratage sans fil ainsi que les outils de sécurité Wi-Fi. 3 exercices pratiques avec des cibles simulées réelles sont proposés.

Module 17 : le piratage des appareils mobiles

Ce module traite des vecteurs d'attaque sur les appareils mobiles, des exploitations des vulnérabilités d'Android ainsi que des directives et outils de sécurité mobile. 5 exercices pratiques avec des cibles simulées réelles sont proposés.

Module 18 : le piratage IoT et OT

Ce module vous apprend à utiliser des techniques de sniffing de paquets pour détecter les failles du réseau, ainsi que des solutions de défense contre les attaques de sniffing. 2 exercices pratiques avec des cibles simulées réelles sont proposés.

Module 19 : le cloud computing

Ce module couvre les concepts du cloud computing comme les technologies de conteneurs et le serverless computing, les diverses menaces et attaques basées sur le cloud, ainsi que les techniques et outils de sécurité du cloud. 5 exercices pratiques avec des cibles simulées réelles sont proposés.

Module 20 : la cryptographie

Ce dernier module CEH vous permet de maîtriser la cryptographie et le chiffrement, ainsi que l'infrastructure à clé publique, les attaques cryptographiques et les outils de crypto-analyse. 2 exercices pratiques avec des cibles simulées réelles sont proposés.

Certification CEH

Examen Certified Ethical Hacker (312-50)

Durée : 4 heures

125 questions à choix multiples

Langue : anglais

Réussite entre 60 et 80% de bonnes réponses

La formation CEH v12 vous permet d'obtenir le titre de Certified Ethical Hacking. Pour l'obtenir, vous devrez dans un premier temps passer 1 examen portant sur vos connaissances. Il consiste à répondre à 125 questions à choix multiples en 4 heures. Par la suite, vous pourrez passer 1 examen facultatif basé sur la pratique. Ce dernier examen consiste à répondre à une série de 20 questions axées sur des mises en situation pendant 6 heures. Il permet d'obtenir le titre de C|EH® (Master)

Avec la nouvelle version C|EH® v12, EC-Council a inclus la possibilité de repasser les examens gratuitement. Cela signifie que vous pouvez repasser vos examens si vous échouez. Cependant, 4 reprises sont autorisées par an conformément à la politique d'examen.

A noter : la certification professionnelle CEH 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).