EC-Council Certified Ethical Hacker (CEH) + Voucher d'examen

Durée: 5 Jours **Réf de cours: CEH** **Version: 12** **Méthodes d'apprentissage: Intra-entreprise & sur-mesure**

Résumé:

Le Certified Ethical Hacker a été mis à l'épreuve au cours des 20 dernières années, créant des centaines de milliers de Certified Ethical Hackers employés par des entreprises, des armées et des gouvernements de premier plan dans le monde entier.
Dans sa 12e version, le Certified Ethical Hacker propose une formation complète, des laboratoires d'apprentissage pratiques, des champs de pratique cybernétiques, des évaluations de certification, des compétitions cybernétiques et des opportunités d'apprentissage continu dans un programme complet conçu à partir de notre nouveau cadre d'apprentissage : 1. Apprendre 2. Certifier 3. S'engager 4. Compétitionner.
Le C|EH v12 permet également aux aspirants professionnels de la cybersécurité d'acquérir les tactiques, techniques et procédures (TTP) nécessaires pour former des hackers éthiques capables de découvrir les faiblesses de presque tous les types de systèmes cibles avant que les cybercriminels ne le fassent.
Mise à jour : 15.05.2023

Cours CEH v12 avec vidéos de formation en français : accès au dernier programme Certified Ethical Hacker (CEH) v12, accompagné de vidéos de formation de haute qualité en langue française.

Formation intra-entreprise

Cette formation est délivrable en session intra-entreprise, dans vos locaux ou dans les nôtres. Son contenu peut être adapté sur-mesure pour répondre aux besoins de vos collaborateurs. Contactez votre conseiller formation Global Knowledge ou adressez votre demande à info@globalknowledge.fr.

Public visé:

La formation Certified Ethical Hacking sera très utile aux responsables de la sécurité, aux auditeurs de la cybersécurité, aux professionnels de la sécurité, aux administrateurs de sites, aux analystes de la sécurité et à toute personne concernée par l'intégrité de l'infrastructure du réseau.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Effectuer un footprinting et une reconnaissance en utilisant les dernières techniques de footprinting, y compris le footprinting à travers les services Web et les sites de réseautage social et les outils en tant que phase critique de pré-attaque requise dans le piratage éthique.
- Utiliser les techniques de balayage du réseau et contre-mesures de balayage ainsi que les techniques d'énumération et contre-mesures d'énumération
- Analyser des vulnérabilités pour identifier les failles de sécurité dans le réseau, l'infrastructure de communication et les systèmes finaux de l'organisation cible
- Comprendre la méthodologie de piratage des systèmes, stéganographie, attaques par stéganalyse et pistes de couverture pour découvrir les vulnérabilités des systèmes et des réseaux
- Identifier les différents types de menaces liées aux logiciels malveillants (chevaux de Troie, virus, vers, etc.), audit des systèmes pour les attaques de logiciels malveillants, analyse des logiciels malveillants et contre-mesures
- Présenter l'ensemble des technques pour parer les différentes attaques
- Expliquer le cryptage sans fil, méthodologie de piratage sans fil, outils de piratage sans fil et outils de sécurité Wi-Fi.
- Vecteur d'attaque des plateformes mobiles, exploitation des vulnérabilités d'android, directives et outils de sécurité mobile
- Identifier les menaces pour les plateformes IoT et OT et apprendre à défendre les dispositifs IoT et OT en toute sécurité.
- Chiffres de cryptographie, infrastructure à clé publique (PKI), chiffrement des courriels, attaques de cryptographie et contre-mesures en cas d'attaque de cryptographie.

Pré-requis:

- Avoir deux ans d'expérience en sécurité informatique et posséder une connaissance de base de Linux et/ou Unix.
- Familiarité avec les concepts de cybersécurité
- Une solide connaissance pratique de : TCP/IP, Windows Server

Test et certification

Cette formation est recommandée comme préparation à l'examen suivant :

312-50 - Hacker éthique certifié

Contenu:

Module 01

- Introduction à l'Ethical Hacking
- Couvrir les fondamentaux des questions clés dans le monde de la sécurité de l'information, y compris les bases du piratage éthique, les contrôles de la sécurité de l'information, les lois pertinentes et les procédures standards.

Module 02

- Impression et reconnaissance
- Apprendre à utiliser les techniques et les outils les plus récents pour effectuer des recherches et des reconnaissances, une phase pré-attaque critique du processus de piratage éthique.

Module 03

- Analyse des réseaux
- Apprendre les différentes techniques d'analyse des réseaux et les contre-mesures.

Module 04

- Enumération
- Apprendre différentes techniques d'énumération, telles que les exploits Border Gateway Protocol (BGP) et Network File Sharing (NFS), et les contre-mesures associées.

Module 05

- Analyse des vulnérabilités
- Apprendre à identifier les failles de sécurité dans le réseau, l'infrastructure de communication et les systèmes finaux d'une organisation cible. Différents types d'évaluation des vulnérabilités et d'outils d'évaluation des vulnérabilités.

Module 06

- Piratage de système
- Apprendre les différentes méthodologies de piratage de système utilisées pour découvrir les vulnérabilités du système et du réseau.

Module 07

- Menaces liées aux logiciels malveillants
- Apprendre les différents types de logiciels malveillants (chevaux de Troie, virus, vers, etc.), les APT et les logiciels malveillants sans fichier, la procédure d'analyse des logiciels malveillants et les contre-mesures aux logiciels malveillants.

Module 08

- "Reniflage"
- Apprendre les techniques de "reniflage" de paquets et comment les utiliser pour découvrir les vulnérabilités du réseau, ainsi que les contre-mesures pour se défendre contrece type d'attaques.

Module 09

- Ingénierie sociale
- Apprendre les concepts et les techniques d'ingénierie sociale, y compris comment identifier les tentatives de vol, auditer les vulnérabilités au niveau humain, et suggérer des contre-mesures d'ingénierie sociale.

Module 10

- Déni de service
- Apprendre les différentes techniques d'attaques par déni de service (DoS) et par déni de service distribué (DDoS), ainsi que les outils utilisés pour auditer une cible et concevoir des contre-mesures et des protections DoS et DDoS.

Module 11

- Détournement de session
- Comprendre les différentes techniques de détournement de session utilisées pour décourager la gestion de session au niveau du réseau, l'authentification, l'autorisation et les faiblesses cryptographiques, ainsi que les contre-mesures associées.

Module 12

- Éviter les IDS, les Firewalls et les Honeypots
- Introduction aux techniques d'évasion des pare-feu, des systèmes de détection d'intrusion (IDS) et des pots de miel, aux outils utilisés pour auditer le périmètre d'un réseau à la recherche de faiblesses et aux contre-mesures.

Module 13

- Piratage des serveurs web
- Apprendre les attaques de serveurs web, y compris une méthodologie d'attaque complète utilisée pour vérifier les vulnérabilités dans les infrastructures de serveurs web et les contre-mesures.

Module 14

Module 15

- Injection SQL
- Apprendre les attaques par injection SQL, les techniques d'évasion et les contre-mesures à l'injection SQL.

Module 16

- Piratage des réseaux sans fil
- Comprendre les différents types de technologies sans fil, y compris le cryptage, les menaces, les méthodologies de piratage, les outils de piratage, les outils de sécurité Wi-Fi et les contre-mesures.

Module 17

- Piratage des plateformes mobiles
- Apprendre les vecteurs d'attaque des plateformes mobiles, le piratage d'Android et d'iOS, la gestion des appareils mobiles, les directives de sécurité mobile et les outils de sécurité.

Module 18

- Piratage de l'IoT
- Apprendre les différents types d'attaques IoT et OT, la méthodologie de piratage, les outils de piratage et les contre-mesures.

Module 19

- Informatique dans le Cloud
- Apprendre les différents concepts de l'informatique dans le Cloud, tels que les technologies de conteneurs et l'informatique sans serveur, les différentes menaces, les attaques, la méthodologie de piratage et les techniques et outils de sécurité.

Module 20

- Cryptographie
- Apprendre les algorithmes de cryptage, les outils de cryptographie, l'infrastructure à clé publique (PKI), le cryptage des courriels, le cryptage des disques, les attaques de cryptographie et les outils de cryptanalyse.

Ateliers pratiques

- Avec plus de 220 laboratoires pratiques réalisés dans notre environnement cybernétique, vous aurez l'occasion de mettre en pratique chaque objectif d'apprentissage sur des machines réelles et des cibles vulnérables dans le cours.
- Préchargé avec plus de 3 500 outils de

- Piratage des applications web
- Apprendre les attaques des applications web, y compris une méthodologie complète de piratage des applications web utilisée pour auditer les vulnérabilités des applications web et les contre-mesures.

piratage et divers systèmes d'exploitation, vous obtiendrez une exposition sans précédent et une expérience pratique avec les outils de sécurité les plus courants, les dernières vulnérabilités et les systèmes d'exploitation les plus répandus dans l'industrie.

- Notre gamme est accessible sur le web, ce qui vous permet d'apprendre et de pratiquer de n'importe où.

Méthodes pédagogiques :

Support de cours officiel remis aux participants

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement