

Mis à jour le 23/04/2025

S'inscrire

Formation CEH™ - Certified Ethical Hacker™

Examen inclus + 1 an d'accès

5 jours (35 heures)

Présentation

Notre formation [Certified Ethical Hacker](#) vous préparera au passage de la certification "Certified Ethical Hacker". Assimiler les connaissances nécessaires pour sécuriser les systèmes réseau, les bases de données ou encore les attaques de hacker.

Le cours en est maintenant à sa 13e version, il a été mis à jour afin de vous apporter les outils et techniques utilisés par les pirates et les professionnels de la sécurité, susceptibles de pénétrer dans n'importe quel système d'information.

Grâce à la formation CEH™ vous plongerez dans l'état d'esprits des hackers afin de vous prémunir de toute attaque. La certification CEH™ accréditée en conformité ANSI 17024 vous permettra de tester, scanner, et hacker un système visé.

Avec Ambient IT en tant qu'organisme de formation, profitez du pack CEH™ Elite, inclus avec votre préparation.

Contenu de la formation

- 1 an d'accès aux cours en ligne eCourseware
- 6 mois d'accès aux Labs
- 1 Voucher de passage à l'examen
- 1 retake de l'examen (en cas d'échec)
- CEH Engage (test et préparation)
- Global CEH Challenges (pass annuel pour les compétitions)
- CEH Practical Exam
- 10 vidéos d'apprentissage de la cybersécurité

Objectifs

- Comprendre les fondamentaux du hacking éthique
- Avoir les compétences pour sécuriser les systèmes, les réseaux, les bases de données ou les applications des attaques de hacking
- Être prêt pour passer la certification CEH™

Public visé

- Hackers éthiques
- Expert en sécurité informatique
- Développeurs
- Administrateurs
- Administrateur réseaux

Pré-requis

- Expérience en utilisation de système d'exploitation Windows et Linux
- Connaissance basique des protocoles et du fonctionnement des réseaux TCP/IP
- 2 ans d'expérience en cybersécurité

Ambient IT n'est pas ATC d'EC-Council. CEH™ est une marque déposée par EC-Council international limited. Ambient IT n'est ni affilié, ni accrédité par EC-Council.

Programme de la Préparation à la Certification CEH™

Introduction

- Retour sur les bases de la sécurité
- Qu'est-ce que le hacking éthique ?
- Quelles sont les missions du hacker éthique ?

Collecte d'informations

- Footprinting
- Réseaux TCP/IP
- Méthode de scannage
- Énumération

Attaque des réseaux

- Wireless networking
- Les concepts réseau
- Les techniques et les outils

- Les techniques d'évasion
- Wireless hacking

Hacker un système

- Authentification
- Élévation des privilèges
- Cacher les fichiers
- Couvrir ses traces
- Les logiciels malveillants
- Déni de service
- Détournement de session
- Hacker une application web

Les serveurs web

- Les méthodologies d'attaques
- Architecture serveur Web
- Les attaques serveur
- Les attaques contre les applications web

IoT

- Architecture
- La méthode pour hacker
- Les vulnérabilités
- Les attaques
- Les attaques et les vulnérabilités mobiles

Cloud Computing

- Les types de services
- Les menaces
- Les attaques
- Cloud hacking

Cryptographie

- Rappel sur la cryptographie
- PKI
- Certificats digitaux
- Communications cryptées
- Attaques cryptographiques

Pentest

- Audit de sécurité
- Reconnaissance active
- La méthodologie
- Exploitations

Social Engineering

- Présentation de l'ingénierie sociale
- Se protéger contre ce type d'attaque
- Attaques contre les mobiles vs attaques contre les mobiles
- La sécurité physique

Intelligence Artificielle et CyberSécurité

- Overview des différents outils IA
- Menaces Deepfake
- IA et machine learning dans la cybersécurité
- Calcul quantique

Bien se préparer à l'examen CEH

- Présentation de la certification
- Astuces et gestion du temps
- Mémo

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.