

CEH v13 — Certified Ethical Hacker

Réf. CEH · EC-Council · Cybersécurité · **Formation certifiante**

DURÉE	NIVEAU	MODALITÉS	VOUCHER EXAMEN
5 jours	Avancé	Présentiel · Live · Intra	Inclus

Présentation

Le programme CEH v13 d'EC-Council forme aux méthodologies de piratage éthique à travers 20 domaines et des labs immersifs, en intégrant pour la première fois l'IA à chaque phase de l'attaque. Destinée aux professionnels de la sécurité, elle prépare à anticiper, détecter et neutraliser les menaces en pensant comme un attaquant.

Objectifs pédagogiques

- Conduire une reconnaissance et un scan de réseaux avec des outils offensifs
- Exploiter des vulnérabilités systèmes, applicatives et web (OWASP)
- Réaliser des attaques sur les réseaux sans fil, le cloud et l'IoT
- Mettre en œuvre l'ingénierie sociale et les techniques d'évasion
- Utiliser l'IA pour accélérer et automatiser les phases de test d'intrusion
- Rédiger un rapport de pentest et recommander des contre-mesures

Programme détaillé

1. Module 1 — Fondamentaux et reconnaissance

- Introduction au ethical hacking et cyber kill chain
- Footprinting et reconnaissance
- Scanning de réseaux
- Énumération des cibles

2. Module 2 — Vulnérabilités et compromission système

- Analyse de vulnérabilités
- System hacking et élévation de privilèges
- Malwares, chevaux de Troie et backdoors
- Techniques de dissimulation des traces

3. Module 3 — Réseaux, sniffing et social engineering

- Sniffing et interception de trafic
- Ingénierie sociale
- Attaques par déni de service (DoS/DDoS)
- Détournement de session

4. Module 4 — Applications web et bases de données

- Contournement des IDS, pare-feux et honeypots
- Hacking de serveurs et d'applications web
- Injection SQL
- Vulnérabilités OWASP Top 10

5. Module 5 — Sans fil, mobile, IoT et cloud

- Hacking des réseaux Wi-Fi
- Plateformes mobiles
- IoT et OT
- Sécurité et attaques du cloud

6. Module 6 — Cryptographie et IA offensive

- Cryptographie et stéganographie
- Intégration de l'IA dans le pentest
- Méthodologie et reporting
- Contre-mesures et remédiation

Prérequis

Disposer d'au moins 2 ans d'expérience en sécurité de l'information ou avoir suivi une formation réseau/sécurité équivalente. De bonnes connaissances TCP/IP et des systèmes Windows/Linux sont nécessaires.

Public visé

Analystes sécurité, pentesters, administrateurs sécurité, auditeurs, responsables SOC et professionnels souhaitant évoluer vers le ethical hacking.

Ce qui est inclus

- Kit officiel EC-Council (courseware + iLabs)
- Accès aux labs de piratage éthique
- Voucher d'examen CEH inclus
- Attestation de réussite
- Pauses-café, déjeuner et formateur expert certifié

Certification

Certification CEH (examen 312-50) : QCM de 125 questions à passer en 4 heures. Une épreuve pratique optionnelle CEH (Practical) de 6 heures permet d'obtenir le titre CEH Master. Advancia Training est centre d'examen agréé Pearson VUE / PSI.

1 900 DT HT / participant — tarif inter-entreprise · financement CNFCCP possible