MÉTIER DÉVELOPPEUR

CEH
Certified Ethical Hacker

Cette formation propose aux stagiaires, avec l'accès intensif aux labs, de comprendre comment fonctionne la défense périmétrique avant de scanner, tester et hacker son propre système et réseau

Jour 1

Module 1 : Introduction to Ethical Hacking
Module 2 : Footprinting and Reconnaissance
Module 3 : Scanning Networks
Module 4 : Enumeration

Jour 2

Module 5 : Vulnerability Analysis
Module 6 : System Hacking
Module 7 : Malware Threats
Module 8 : Sniffing

Jour 3

Module 9 : Social Engineering
Module 10 : Denial-of-service
Module 11 : Session Hijacking
Module 12 : Evading IDS, Firewalls, and Honeypots

Jour 4

Module 13 : Hacking Web Servers
Module 14 : Hacking Web Applications
Module 15 : SQL Injection
Module 16 : Hacking Wireless Networks

Jour 5

Module 17 : Hacking Mobile Platforms
Module 18 : IoT Hacking
Module 19 : Cloud Computing
Module 20 : Cryptography

Examen « CEH 312-50 » (4 heures, 125 questions à choix multiple en anglais – score minimum 70%)
L'examen peut être passé en ligne dans les locaux de Phosforea à l'issue de la formation. D'une manière générale, il est recommandé de passer l'examen rapidement.

PRÉSENTIEL

35H / 5 JOURS

CEH

OBJECTIFS

• Eduquer, introduire et démontrer des outils de piratage dans le seul but de l'apprentissage des outils et méthodes utilisés par les pirates informatiques.

• Apprendre comment les intrus acquièrent des privilèges et quelles actions peuvent être mises en œuvre afin de sécuriser un système.

PRÉREQUIS

Connaissances basiques des systèmes d'exploitation Windows et Linux et des protocoles réseaux
Connaissances pratiques des protocoles réseaux, menaces web et équipements réseau et sécurité
Compréhension de l'anglais technique (les cours et l'examen sont en anglais)

PUBLIC CIBLE

Ingénieur sécurité
Analyste sécurité
Administrateur système/réseau
Développeur

EC-Council

FORMATION CERTIFIANTE