

Ethical Hacker

Certification CEH - Certified Ethical Hacker

Introduction

Un hacker éthique certifié est un professionnel qualifié qui comprend et sait comment rechercher les faiblesses et les vulnérabilités des systèmes cibles. Pour cela, il utilise les mêmes connaissances et outils qu'un hacker malveillant, mais d'une manière légale et légitime pour évaluer la sécurité d'un système cible.

Cette formation présente une méthodologie de piratage éthique dans le but de découvrir d'éventuelles failles d'un système et de les corriger. Elle permet d'acquérir des compétences en piratage éthique, notamment comment scanner, tester, hacker et sécuriser un système cible. Elle couvre les 5 phases de l'Ethical Hacking : Reconnaissance, Obtention d'accès, Enumération, Maintien de l'Accès et Disparition des traces. Elle présente les outils et techniques de chacune de ces 5 phases.

La formation prépare également à l'examen de certification « CEH - Certified Ethical Hacker ». Cette accréditation certifie les professionnels dans la discipline du piratage éthique pour assurer la sécurité des réseaux et ce, d'un point de vue neutre vis-à-vis des fournisseurs. Pour être admis à l'examen, il faut pouvoir justifier d'au moins 2 ans d'expérience dans le domaine de la sécurité de l'information. L'admission se fait sur la base d'un dossier à soumettre au EC-Council (International Council of E-Commerce Consultants). Les frais d'admission s'élèvent à USD 100.- et la taxe de l'examen à USD 1'199.- (tarifs 2019). L'examen, d'une durée de 4 heures, comprend 125 questions à choix multiple en anglais. L'ISEIG, centre de test Pearson-VUE offre cet examen.

Pour qui

- security officer
- auditor
- security professional
- site administrator
- toute personne concernée par l'intégrité d'une infrastructure réseau

Objectifs

- maîtriser une méthodologie de piratage éthique
- apprendre à scanner, tester, hacker et sécuriser un système cible
- connaître les 5 phases de l'Ethical Hacking et les méthodes et outils à utiliser
- se préparer à l'examen de certification « CEH - Certified Ethical Hacker »

Prérequis

- bonnes connaissances de TCP/IP, Windows Server et Linux
- avoir les prérequis définis par le EC-Council pour être admis(e) à l'examen de certification CEH, soit 2 ans d'expérience dans le domaine de la sécurité de l'information; cette admission se fait sur la base d'un dossier (frais d'admission : USD 100.-)
- bonnes connaissances de l'anglais technique, la documentation pédagogique et l'examen de certification étant en anglais

Ressources

- cours dispensé en français sur la base d'un support de cours officiel en anglais
- 20% d'exercices pratiques
- 1 PC par personne avec environnement virtuel

Programme de la formation

- **Introduction**
 - Rappel TCP/IP / Réseau Matériel
 - Protos / OSI - Adressage IP
- **Introduction à la veille**
 - Vocabulaire
 - BDD de Vulnérabilités et Exploits (attaques non éthiques)
 - Informations générales
- **Prise d'information**
 - Informations publiques
 - Moteur de recherche
 - Prise d'information active
- **Scan et prise d'empreinte**
 - Énumération des machines
 - Scan de ports
 - Prise d'empreinte du système d'exploitation
 - Prise d'empreinte des services
- **Attaques réseau**
 - Idle Host Scanning
 - Sniffing réseau
 - Spoofing réseau
 - Hijacking
 - Attaques des protocoles sécurisés
 - Déni de service
- **Attaques système**
 - Scanner de vulnérabilités
 - Exploitation d'un service vulnérable distant
- Elévation de privilèges
- Espionnage du système
- Attaques via un malware
 - Génération d'un malware avec Metasploit; Encodage de payloads
 - Méthode de détection
- **Attaques Web**
 - Cartographie du site et identification des fuites d'information
 - Failles PHP (include, fopen, Upload, etc.)
 - Injections SQL
 - Cross-Site Scripting (XSS)
 - Cross-Site Request Forgery (CSRF)
 - Bonnes pratiques
- **Attaques applicatives**
 - Escape shell
 - Buffer overflow sous Linux
 - Architecture Intel x86
 - Registres
 - Pile et son fonctionnement
 - Présentation des méthodes d'attaques standards : écrasement de variables, contrôle EIP, exécution d'un shellcode, prise de contrôle du système en tant qu'utilisateur root
- **Préparation à l'examen**

Durée et prix

Formation	Jours	CHF	CHF/j
Ethical Hacker, certification CEH - Certified Ethical Hacker	5	3'750.-*	750.-*

selon conditions générales. Le prix comprend toute la documentation distribuée.

Le cours se déroulent de 13 h 00 à 17 h 00

* Remise de 5 % au membre ADI, GRI, au diplômé(e) ISEIG CPF, titulaire du BFI, DFI ou certifié(e) MCSA, MCSE, MCSD formé(e) à l'ISEIG

