RÉUSSIR VOTRE CERTIFICATION - CEHV12

Préparation à l'Examen en Cinq jours

Du 2 au 6 Octobre 2023

CENTRE DE FORMATION A TUNIS

Introduction

Le Certified Ethical Hacker (C|EH v12) est une formation reconnue et respectée, dont chaque professionnel de la sécurité aura besoin.

Le Certified Ethical Hacker a été lancé depuis 20 années et a été continuellement amélioré et mis à jour, créant des centaines de milliers de Certified Ethical Hackers employés par les plus grandes entreprises, les armées et les gouvernements du monde entier.

Dans sa 12ième version, le Certified Ethical Hacker propose une formation complète, des laboratoires d'apprentissage pratiques, des cybergammes pratiques pour l'engagement, des évaluations de certification, des cyberconcours et des opportunités d'apprentissage continu dans un programme complet organisé par un nouveau cadre d'apprentissage : 1. Apprendre 2. Certifier 3. Engager 4. Concourir.

Ce cours officiel CEH Ethical Hacker v12 de EC-Council aborde 20 modules successifs liés aux domaines de la sécurité informatique les plus récents, en détaillant les dernières techniques de hacking.

Le C|EH v12 équipe également les aspirants professionnels de la cybersécurité avec les tactiques, techniques et procédures (TTP) pour créer des pirates éthiques qui peuvent découvrir les faiblesses de presque tous les types de systèmes cibles avant que les cybercriminels ne le fassent.

Objectifs de la Formation

La formation permet à tous les informaticiens et tous les passionnés d'informatique ayant un profil technique de découvrir et de mieux comprendre les modes opératoires, les méthodes employées ainsi que les différents outils utilisés par les pirates informatiques pour contourner et déjouer les protections de sécurité en place.

Après la formation, le stagiaire aura acquis des connaissances et une expérience réelle en Ethical Hacking

Méthodologie :

Cette formation va permettre aux participants de maitriser une méthodologie de piratage éthique qui pourra aussi bien être utilisée dans un test d'intrusion que dans une situation de piratage éthique et de leur transmettre une vision étendue des variétés d'attaques possibles dans un SI

Les participants seront amenés d'abord à comprendre comment fonctionne la défense périmétrique avant de scanner et d'attaquer leurs propres réseaux. Ils apprendront ensuite comment les intrus acquièrent des privilèges et quelles actions peuvent être mises en œuvre pour sécuriser un système.

Le programme de formation C|EH® v12 comprend 20 modules couvrant diverses technologies, tactiques et procédures, fournissant aux futurs pirates éthiques les connaissances de base nécessaires pour prospérer

dans la cybersécurité. Livrée dans le cadre d'un plan de formation soigneusement organisé qui s'étend généralement sur cinq jours, la 12e version du C|EH® continue d'évoluer pour suivre les derniers systèmes d'exploitation, exploits, outils et techniques.

Les concepts couverts dans le programme de formation sont répartis à 50/50 entre une formation basée sur les connaissances et une application pratique via notre gamme cyber. Chaque tactique abordée dans la formation est soutenue par des laboratoires étape par étape menés dans un environnement virtualisé avec des cibles réelles, des outils actifs et des systèmes vulnérables. Grâce à notre technologie de laboratoire, chaque participant bénéficiera d'une pratique pratique complète pour apprendre et appliquer ses connaissances.

Ce cursus va vous permettre d'obtenir l'examen de certification final CEH Certified Ethical Hacker.

Contenu de la formation

La formation se compose de 20 modules complémentaires et indépendants qui vous aident à maîtriser les fondements du Hacking Ethique et vous préparent préparation à l'examen de certification C|EH comme suit :

- Module 1: Introduction to Ethical Hacking
  Couvrir les principes fondamentaux des problèmes clés du monde de la sécurité de l'information, y compris les bases du piratage éthique, les contrôles de sécurité de l'information, les lois pertinentes et les procédures standard.
- Module 2: Footprinting and Reconnaissance
  Apprendre à utiliser les dernières techniques et outils pour effectuer une empreinte et une reconnaissance, une phase critique de la pré-attaque du processus de piratage éthique.
- Module 3: Scanning networks
  Apprendre différentes techniques d'analyse de réseau et contre-mesures
- Module 4: Enumeration
  Apprendre diverses techniques d'énumération, telles que les exploits du Border Gateway Protocol (BGP) et du Network File Sharing (NFS), ainsi que les contre-mesures associées.
- Module 5: Vulnerability Analysis
  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 de la vulnérabilité et d'outils d'évaluation de la vulnérabilité.
- Module 6: System Hacking
  Découvrir les différentes méthodologies de piratage du système, y compris la stéganographie, les attaques de stéganalyse et les pistes de couverture, utilisées pour découvrir les vulnérabilités du système et du réseau.
- Module 7: Malware Threats
  Découvrir les différents types de logiciels malveillants (cheval de Troie, virus, vers, etc.), les logiciels malveillants de type APT et sans fichier, la procédure d'analyse des logiciels malveillants et les contre-mesures des logiciels malveillants.
- Module 8: Sniffing
  Découvrir les techniques de reniflage de paquets et comment les utiliser pour découvrir les vulnérabilités du réseau, ainsi que les contre-mesures pour se défendre contre les attaques de

reniflage.

- Module 9: Social Engineering
  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: Denial of Service
  Découvrir les différentes techniques d'attaque par déni de service (DoS) et déni de service distribué (DDoS), ainsi que les outils utilisés pour auditer une cible et concevoir des contre-mesures et des protections pour DoS et DDoS.
- Module 11: Session Hijacking
  Comprendre les différentes techniques de piratage de session utilisées pour découvrir la gestion de session au niveau du réseau, l'authentification, l'autorisation et les faiblesses cryptographiques et les contre-mesures associées.
- Module 12: Evading IDS, Firewalls and Honeypots
  S'initier au pare-feu, au système de détection d'intrusion (IDS) et aux techniques d'évasion du pot de miel ; les outils utilisés pour auditer un périmètre de réseau à la recherche de faiblesses ; et contre-mesures.
- Module 13: Hacking Web Servers
  Découvrir les attaques de serveurs Web, y compris une méthodologie d'attaque complète utilisée pour auditer les vulnérabilités des infrastructures de serveurs Web et les contre-mesures.
- Module 14: Hacking Web Applications
  En savoir plus sur les attaques d'applications Web, y compris une méthodologie complète de piratage d'applications Web utilisée pour auditer les vulnérabilités des applications Web et les contre-mesures
- Module 15: SQL Injection
  Découvrir les attaques par injection SQL, les techniques d'évasion et les contre-mesures d'injection SQL.
- Module 16: Hacking Wireless Networks
  Comprendre les différents types de technologies sans fil, y compris le chiffrement, les menaces, les méthodologies de piratage, les outils de piratage, les outils de sécurité Wi-Fi et les contre-mesures.
- Module 17: Hacking Mobile Platforms
  Apprendre le vecteur d'attaque de la plate-forme mobile, le piratage Android et iOS, la gestion des appareils mobiles, les directives de sécurité mobile et les outils de sécurité.
- Module 18: IoT and OT Hacking
  Découvrir différents types d'attaques IoT et OT, la méthodologie de piratage, les outils de piratage et les contre-mesures.
- Module 19: Cloud computing
  Apprendre différents concepts de cloud computing, tels que les technologies de conteneurs et l'informatique sans serveur, diverses menaces de cloud computing, les attaques, la méthodologie de piratage et les techniques et outils de sécurité cloud.
- Module 20: Cryptography
  Découvrir les algorithmes de chiffrement, les outils de chiffrement, l'infrastructure à clé publique (PKI), le chiffrement des e-mails, le chiffrement de disque, les attaques de chiffrement et les outils de cryptanalyse.

Formateur

Anis FOURATI, Tunisien de nationalité, certifié CEH , ISO 27001 LA et ISO 27005 RM, est Expert Auditeur certifié de l'Agence Nationale de la Sécurité Informatique (ANSI). Disposant de plus de 20 ans d'expérience professionnelle, il intervient principalement sur les missions d'audit technique, de sécurité des systèmes d'information et des tests intrusifs. Anis FOURATI est Certifié EC COUNCIL et PECB trainer.

Pré-requis

Connaissances professionnelles de TCP/IP, Linux et Windows Server

Public visé

La formation et l'examen CEH v12 s'adressent aux :

- Responsables sécurité
- Auditeurs de la sécurité
- Professionnels de la sécurité
- Administrateurs de site
- Toute personne concernée par la stabilité des systèmes d'information

Informations Générales sur l'examen

- Titre de l'examen : Certified Ethical Hacker v12
- Code de l'examen : 312-50
- Format de l'examen : QCM
- Type de l'examen : CBT – En ligne
- Nombre de questions: 125
- Score requis: de 70% à 78% (QCM) selon la complexité des questions
- Langue: anglais
- Durée : 4 heures
- Lieu de l'examen: les locaux de BIT ou centre VUE

Ressources

- Support de cours officiel en anglais
- Cours donné en français
- 20% d'exercices pratiques
- 1 PC par personne / Internet
- des Q/R pour s'entrainer