

CERTIFIED ETHICAL HACKER v9 (CEH v9)

OBJECTIFS DE LA FORMATION

Cette formation vous permettra de maîtriser une méthodologie et les techniques de piratage éthique, qui pourront être utilisées pour les tests d'intrusion externe (site web, infrastructure...) ainsi que pour les tests d'intrusion interne (LAN...). Vous quitterez le cours avec des compétences en piratage éthique qui sont hautement recherchées, tout comme, globalement, la certification Certified Ethical Hacker!

CONTENU DE LA FORMATION

INTRODUCTION TO ETHICAL HACKING

- > Vue générale de la sécurité, des menaces et des vecteurs d'attaques
- > Concepts, types et phases de hacking
- > Concept et portée de l'Ethical Hacking
- > Notions de contrôles de sécurité
- > Initiation à la législation et aux standards liés à la sécurité

FOOTPRINTING AND RECONNAISSANCE

- > Concepts de footprint
- > Méthodologie de reconnaissance : navigateurs, techniques Advanced
- > Google Hacking, réseaux sociaux, sites web, e-mail, veille concurrentielle, WHOIS, DNS, réseau, social engineering
- > Outils et Contre-mesures

SCANNING NETWORKS

- > Vue générale du scanning de réseau
- > Méthodologie CEH : live systems, Open ports, scanning sous IDS, accaparement de bannière, scan de vulnérabilité, tracer un diagramme de réseau, préparer les proxys

SYSTEM HACKING

- > Informations disponibles avant l'étape de hacking de système
- > Les objectifs du hacking de système
- > Méthodologie CEH
- > Etapes de hacking de système
- > Fichiers cachés / Effacer ses traces

MALWARE THREATS

- > Introduction aux malwares
- > Chevaux de Troie : concepts, types Virus et vers : étapes, types, signaux d'alerte, ransomwares,
- > Détection de malwares
- > Contre-mesures
- > Logiciels anti malwares



INFORMATIONS GÉNÉRALES

RÉF. : **FORCEHv9**

DURÉE : 5 jours de 7H, soit 35H de formation

COÛT : nous consulter

LIEU : Sainte Marie OU Saint Denis, La Réunion

CODE CPF tout public : **En cours d'attribution**

PRÉ REQUIS

Des connaissances basiques de TCP-IP, Linux et Windows Server sont nécessaires pour suivre ce cours.

PUBLIC VISÉ

- > Responsable de la sécurité des systèmes d'informations (RSSI)
- > Administrateurs système et réseaux
- > Auditeurs
- > Développeurs
- > Pentesteurs juniors
- > Responsable informatique

NOTRE FORMATEUR

La formation est dispensée par un consultant de la société Sysdream, qui est le centre ATC officiel d'EcCouncil autorisé à dispenser cette formation.

MOYENS PÉDAGOGIQUES, TECHNIQUES ET D'ENCADREMENT

La formation vous donne accès à :

- > Une salle équipée et climatisée (paper-board, tableau blanc, vidéo projecteur, postes informatiques ...)
- > Supports de cours officiels du formateur
- > Une connexion internet
- > Certification à la fin de la formation incluse



CERTIFIED ETHICAL HACKER v9 (CEH v9)

SNIFFING / SOCIAL ENGINEERING

- > Concepts de sniffing
- > Différents types d'attaques : attaques sur Mac, attaques DHCP, ARP, Spoofing infection de DNS
- > Outils de détection
- > Contre-mesures
- > Techniques de détection

DENIAL OF SERVICE

- > Concepts d'ingénierie sociale
- > Techniques d'ingénierie sociale
- > Usurpation d'identité sur les réseaux sociaux
- > Procédure d'usurpation d'identité
- > Contre-mesures d'ingénierie sociale

SESSION HIJACKING

- > Concepts de DpS/DDoS
- > Techniques d'attaques de DpS/DDoS
- > Étude de cas de DDoS / Outils d'attaques DoS/DDoS
- > Contre-mesures/ Outils de protection DoS/DDoS

HACKING WEB APPLICATIONS

- > Concepts et attaques de serveurs web
- > Méthodologie et outils d'attaque

HACKING WIRELESS NETWORKS

- > Concepts du sans-fil/ Chiffrement pour le wireless
- > Menaces liées au réseau wireless
- > Méthodologie d'attaque de réseau sans fil
- > Outils de hacking de réseau sans fil
- > Hacking de Bluetooth/ Contre-mesures

HACKING MOBILE PLATFORMS

- > Vecteurs d'attaques de plateformes mobiles
- > Hacking Android OS / iOS / Windows Phone / Blackberry
- > Mobile Device Management (MDM) : solutions de MDM, BYOD
- > Outils et lignes directrices de sécurité mobile

CLOUD COMPUTING

- > Introduction au Cloud Computing
- > Menaces liées au Cloud Computing
- > Attaques dans le cloud
- > Sécurité dans le cloud
- > Outils de sécurité pour le cloud

