Microtel
Training institute

CERTIFIED ETHICAL HACKER

CURSUS:
EC-COUNCIL

CODE DE LA FORMATION:
EC-SC-CEH

VERSION:
10

DURÉE:
5 JOURS

La formation CEH v10 est la plus avancée au monde en matière de piratage éthique. Elle couvre 20 des plus grands domaines que chaque pirate éthique veut connaître pour monter en compétences dans le domaine de la sécurité de l'information.
A travers ces 20 modules, la formation couvre plus de 270 attaques techniques les plus utilisées par les pirates.

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

PUBLIC:
Cette formation Certification Ethical Hacking v10 s'adresse à des Responsables de la sécurité des systèmes d'information, aux Administrateurs de sites, Auditeurs, Responsables informatique et aux décisionnaires ayant besoin de comprendre les solutions qui existent aujourd'hui en matière de sécurité et qui sont concernés par l'intégrité de l'infrastructure réseau.

OBJECTIFS:
L'objectif de ce cours est de vous aider à maîtriser une méthodologie de piratage éthique qui pourra bien être utilisée dans un test d'intrusion.
Ce stage vous apporte des compétences en piratage éthique qui sont hautement recherchées, de même que la certification Certified Ethical Hacker!

CONTENU:

Introduction au 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 contôles de sécurité
- Initiation à la législation et aux standards liés à la sécurité

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

- Reconnaissance dans les tests d'intrusion

Scanning de réseaux

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

Enumération

- Concepts d'énumération
- NetBIOS
- Les différents types d'énumération : SNMP, LDAP, NTP, SMTP
- Contre-mesures d'énumération
- Contre-mesures d'énumération SMB

Analyse des Vulnérabilités

- Introduction à l’analyse des vulnérabilités
- Cycle de vie de l’analyse des vulnérabilités
- Différentes approches et outils utilisés dans l’analyse des vulnérabilités.

Hacking de système

- 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

Malwares

- Introduction aux malwares
- Chevaux de Troie : concepts, types
- Virus et vers : étapes, types, signaux d'alerte, ransonwares, canulars et faux antivirus, différencier un ver et un virus, programmation de virus
- Ingénierie anti malwares
- Détection de malwares
- Contre-mesures
- Logiciels anti malwares

Sniffing

- 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

Ingénierie sociale

- 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

Attaques par Déni de Service

- Concepts de DpS/DDoS
- Techniques d'attaques de DpS/DDoS
- Botnets
- Etude de cas de DDoS
- Outils d'attaques DoS/DDoS
- Contre-mesures

- Outils de protection DoS/DDoS

Détournement de sessions

- Concepts de détournement de session
- détournement de sessions d'applications
- détournement de sessions de réseau
- Outils de détournement de session
- Contre-mesures

Hacking de serveurs Web

- Concepts de serveurs web
- Attaques de serveurs Web
- Méthodologie d'attaque
- Outils d'attaque de serveurs Web
- Contre-mesures
- Gestion des patches
- Ourils de sécurité des serveurs web

Piratage d’applications Web

- Concepts de web app
- Menaces sur les web apps
- Méthodologie d'attaque de web applications
- Outils d'attaque d’applications Web
- Contre-mesures
- Outils de sécurité

Injection SQL

- Concepts d'injections SQL
- Types d'injection SQL
- Méthodologie d'injection SQL
- Outils d'injection SQL
- Techniques d'évasion
- Contre-mesures

Hacking de réseaux sans fil

- Concepts du sans fil
- Chiffrement pour le wireless
- Menaces liées au réseau wireless
- Méthodologie d'attaque de réseau sans fil : wi-fi, GPS, analyse de trafic, lancement d'attaque, craquer le chiffrement wi-fi
- Outils de hacking de réseau sans fil
- Hacking de bluetooth
- Contre-mesures
- Outils de sécurité de réseau sans fil

Hacking de plateformes mobile

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

Evading IDS, Firewalls & Détection de Honey Pots

- Concepts de IDS, Firewall et Honeypot
- Systèmes de IDS, Firewall et Honeypot

- Contourner l'IDS
- Contourner le firewall
- Outils de contournement d'IDS, de firewall
- Détecter les honeypots
- Contre-mesures de contournement d'IDS et de firewal

Hacking IoT (Internet des Objets)

- Introduction à l’Internet des Objets (IoT)
- Menaces liées à l’Internet des Objets (IoT)
- Attaques dans l’Internet des Objets (IoT)
- sécurité dans l’Internet des Objets (IoT)
- Outils de sécurité pour l’Internet des Objets (IoT)

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

Cryptographie

- Concept et état des lieux de la cryptographie
- Algorithmes de chiffrement
- Outils de cryptographie
- Public Key Infrastructure (PKI)
- Chiffrement d'e-mail
- Chiffrement de disque
- Attaques de cryptographie
- Outils de cryptographie

LAB:

Ces labs reprennent des scénarios réels évoqués au cours de la formation afin de percevoir une attaque telle qu'elle se présenterait dans la réalité