

Formation sécurité informatique: Protection contre le piratage (PENCPFR, 4 jours)

Description

Le cours Formation sécurité informatique : Protection contre le piratage est une introduction au white hat hacking. Le cours vous apprend à réaliser chaque étape du processus de piratage afin de pouvoir protéger votre environnement. La formation comprend des outils pour la collecte d'informations et la détermination de la cible, la découverte et l'énumération des cibles, la cartographie des vulnérabilités et l'ingénierie sociale. Vous apprendrez à utiliser le cadre Metasploit pour identifier et exploiter les cibles afin d'éviter que cela ne vous arrive. Le laboratoire pratique progressif et pratique vous permet d'exécuter un piratage depuis l'identification initiale jusqu'à l'escalade des privilèges et la maintenance. Arrêtez les pirates dès aujourd'hui !

Tarifs

- Tarification: \$3,750/person
- Rabais de 10% lorsque vous inscrivez 3 personnes.

Plan de cours

Linux Kali : L'essentiel

Configuration de Linux Kali

Une note sur la configuration du laboratoire

Une introduction rapide à la ligne de commande Linux

Visite du système de fichiers de Linux

Maîtriser les privilèges des utilisateurs et SELinux

Tout sur les autorisations de fichiers

Modifier des fichiers avec VIM

Linux Kali : Quelques sujets utiles

A propos de Runlevels et Boot

Gérer les paquets avec apt-get

Gestion des processus et des services

Configurer et comprendre les adresses IP et les noms d'hôtes

Maîtriser Netcat

Maîtriser le pare-feu

Une visite rapide de TCPDump

Scripting BASH et autres programmations

En savoir plus sur l'édition VIM

Configurer votre profil

Travailler avec des citations

Travailler avec des variables

Mise en œuvre de la logique conditionnelle

Mise en œuvre de la logique de répétition

Quelques concepts plus avancés

Écrire des scripts en Python : Une visite rapide

Introduction aux compilateurs C

Écrire et compiler du code C

Outils puissants : Le cadre Metasploit

Qu'est-ce que le cadre Metasploit ?

Démarrage et mise à jour de Metasploit

Trouver des modules Metasploit

Utilisation des modules Metasploit

Définition des options du module

Travailler avec des charges utiles

Configuration manuelle d'une charge utile

Travailler avec PostgreSQL

Travailler avec msfcli

Utilisation de msfvenom

Aperçu des modules auxiliaires

La phase d'évaluation

Les bases de la collecte de renseignements

Que fournit le balayage des ports ?

Les détails de nmap

Plus d'informations sur nmap Scanning

Travailler avec le moteur de script nmap

Travailler avec des scanners Metasploit

Travailler avec Metasploit Exploit Checking

Configuration de ZAP Attack

Analyse des applications Web avec ZAP Attack

Capturer le trafic réel

Aperçu des outils de capture de réseau

Travailler avec TCPDump

Travailler avec Wireshark

Empoisonnement du cache ARP et DNS

Attaques SSL et déverrouillage SSL

L'art de l'exploitation : Les bases

Exploitation du protocole SMB

Exploitation des partages NFS

Exploitation avec les informations d'identification par défaut de WebDAV

Exploitation et ouverture de phpMyAdmin

Téléchargement de fichiers sensibles

Exploitation d'un dépassement de tampon dans un logiciel tiers

Exploitation d'applications Web tierces

Exploitation d'un service compromis

Exploitation du bureau à distance

L'art de l'exploitation : Applications serveur

Exploitation de SSH

Exploitation d'Apache

Exploitation du serveur Web IIS

Exploitation du FTP

Exploitation de SQL Server

Exploitation d'Oracle

Exploitation de MySQL

Attaques par mot de passe

Gestion des mots de passe

Attaques de mots de passe en ligne

Attaques de mots de passe hors ligne

Extraire les mots de passe en clair de la mémoire avec Windows Credential Editor

Ingénierie sociale

La boîte à outils de l'ingénieur social

Attaques de harponnage

Attaques sur le Web

Attaques par courriels de masse

Attaques multidimensionnelles

Contournement des applications antivirus

Trojans

Comment fonctionnent les applications antivirus

Microsoft Security Essentials

Passer outre un programme antivirus

Se cacher à la vue de tous

Après l'exploitation

Introduction à Meterpreter

Travailler avec les scripts du Meterpreter

Tout sur les modules de post-exploitation de Metasploit

Escalade locale de privilèges

Collecte d'informations locales

Mouvement latéral

Pivotant

Persistance

Test des applications Web

Travailler avec ZAP Attack

Injection SQL

Injection XPath

Inclusion de fichiers locaux

Inclusion de fichiers à distance

Exécution des commandes

Cross-Site Scripting

Falsification de requête intersite

Analyse des applications Web avec w3af

Attaques sans fil

Mise en place

Mode moniteur

Capture des paquets

Sans fil ouvert

Confidentialité équivalente au filaire

Accès protégé Wi-Fi

WPA2

Wi-Fi Protected Setup

Piratage mobile

À propos du cadre du Pentest de Smartphone

Vecteurs d'attaque mobiles

Le cadre du Pentest du Smartphone

Attaques à distance

Attaques côté client

Applications malveillantes

Exploitation des postes mobiles

Exploits avancés (si le temps le permet)

Comprendre les dépassements de tampon

Création du code d'exploitation

Compilation du code d'exploitation

Chargement de la charge utile

Exécution du code

Recueillir des informations et prendre le contrôle