

Formation Linux: Cours complet sur la sécurité et le piratage (UNXHACKFR, 4 jours)

Description

Le cours Formation Linux : Cours complet sur la sécurité et le piratage se concentre sur la sécurité et le piratage de Linux. En commençant par une plongée en profondeur dans la sécurité de Linux, le cours aborde l'anatomie d'une attaque de pirates sur Linux. Chaque partie du système d'exploitation Linux est incluse dans la discussion, y compris le noyau, les composants réseau, les bases de données, les serveurs Web et plus encore.

Tarifs

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

Plan de cours

Sécurité et logiciels malveillants sous UNIX/LINUX

L'anatomie d'une attaque

PDRP : Planifier, Détecter, Répondre, Prévenir.

Sources de menaces

Catégories de menaces

Lutte contre les virus

Lutte contre les vers

Lutte contre les logiciels espions

Faire face aux attaques par courrier électronique

Traitement des scripts malveillants

Qu'en est-il du serveur web et des autres technologies d'accès à distance ?

Qu'en est-il des serveurs d'application ?

Aperçu des mesures et outils de sécurité d'UNIX/LINUX

Le point de vue du hacker sur UNIX/LINUX

À propos de l'authentification et de l'autorisation

Architecture de sécurité

Principes essentiels de sécurité

Un regard sur les royaumes de sécurité

Authentification UNIX/LINUX

Autorisation UNIX/LINUX

À propos de l'audit et de la journalisation

Fonctionnalités et outils

Installation sécurisée par défaut

À propos du super utilisateur

À propos des noms d'utilisateur et des mots de passe

À propos des pare-feu

Modèles de sécurité et configuration de la sécurité

Profilage de base

Utilisation des groupes et des royaumes

A propos du cryptage

Protection des fichiers et des répertoires

Empreinte, analyse et énumération

Les bases de la détection : Le cycle de vie complet

Explorer l'empreinte écologique

Exploration de la numérisation

À propos des noms d'ordinateurs et des adresses IP

Exploration de RPC

Explorer les PME

Approfondir le DNS

Un regard plus attentif sur l'énumération SNMP

Piratage de services

Craquage de mots de passe

Approfondir l'authentification UNIX/LINUX

Craquer l'authentification

Autres services

Escalade et contrôle des privilèges

Prédiction des tuyaux nommés

Demandes NetDDE

Explorer les contre-mesures

Contrôle de la ligne de commande

Contrôle GUI

Extension de l'attaque

Audit

Craquage des mots de passe

À propos des chevaux de Troie

Recherche de fichiers

Capture de paquets

Excursions sur les îles

Nettoyage

Création de comptes d'utilisateurs fictifs

Écrans de connexion des chevaux de Troie

Télécommande

Où sont les portes dérobées et les chevaux de Troie ?

À propos des rootkits

Couvrir vos traces

Couvrir les traces

Contre-mesures générales

Piratage d'Apache

Architecture Apache

Dépassement de tampon

Traversée du système de fichiers

Attaques du code source

Piratage des applications Web

Piratage des clients Internet

Aperçu de l'architecture du navigateur

Comment joindre un client Internet

Attaques déchainées

L'attaque complète

Explorer les contre-mesures

Piratage des bases de données

Défendre Oracle

Meilleures pratiques en matière de sécurité

Piratage de Telnet

À propos de Telnet

Identification et énumération de Telnet

Attaquer Telnet

Contre-mesures générales de Telnet

Autres stratégies d'attaque

Attaquer le SAM

À propos des attaques de systèmes de fichiers

Mise en œuvre des attaques DoS