

EDUCACIÓN 

Seguridad Linux: Server Hacking

Programa de Estudio

Seguridad Linux: Server Hacking

Domina las técnicas para garantizar la seguridad del sistema operativo Linux. Aprende a usar la defensa y los ataques preventivos dentro de tus servidores.



Contenido del curso

El curso de Seguridad Linux está orientado a toda persona que esté interesada en comprender las técnicas y herramientas que pueden utilizarse para aumentar la seguridad de los sistemas operativos GNU/Linux, a fin de protegerlos de diversos tipos de ataque.

Durante las clases realizaremos prácticas sobre las versiones más recientes de las distribuciones Linux más populares, que nos permitirán entrar en contacto directo con las técnicas, herramientas y comportamientos de dichos sistemas.

PRÁCTICAS EN CLASE ::

Se configurarán algunas de las opciones más importantes de seguridad en el sistema operativo, como la política de contraseñas y el bloqueo de cuentas. También aprenderemos a cifrar archivos dentro del sistema, para protegernos de diversos tipos de robos de datos.

Se aprenderá a trabajar con el firewall de Linux, IPTables, a fin de bloquear conexiones no autorizadas, basándonos en varios aspectos, como las direcciones IP de origen y destino, y los puertos TCP

Se analizará cómo implementar la autenticación multi-factor (MFA), para proteger los accesos remotos a los servidores. Por último, estudiaremos cómo se pueden auditar los cambios importantes en el sistema y dejar registro de cualquier acción crítica en el mismo.

Público

Este curso está orientado, a cualquier persona sea un profesional de ciberseguridad, pentester,

desarrollador, implementador ISO, auditor, así como para entusiastas de la tecnología.

Salida Laboral

Al finalizar el curso te convertirás en un operador en Seguridad Linux, como SysAdmin y DevOps.

Requisitos

Conocimientos previos: Tener conocimientos de seguridad informática o haber realizado el curso de Introducción a la seguridad Informática Tener conocimientos de criptografía o haber realizado el curso de Criptografía y Blockchain Tener conocimientos de seguridad en redes o haber realizado el curso de Seguridad en Redes: Network Hacking Tener conocimientos de seguridad en Administración Linux o haber realizado el curso de Linux Administrador Recomendable: Tener conocimientos de Ethical hacking o haber realizado el curso de Ethical Hacking

Modalidad de cursado

Puedes tomar este curso en modalidad presencial o modalidad online - en vivo

¿Qué aprenderás?

- Configuración de seguridad en arranque
- Seguridad para contraseñas y cuentas de usuarios
- Mitigar ataques Dos/DDos con reglas IPTables
- Agregar y eliminar reglas
- Detección de intrusos
- Monitoreo de sistemas de archivos
- Autenticación Multi-Factor
- Manejo de Knockd y Auditd
- Protección de datos confidenciales con cifrado de Volúmenes de Disco
- Filtro de tráfico: protocolos, puertos y direcciones IP
- Cómo identificar un malware oculto en el sistema
- Accesos físicos y remotos: protección de ataques
- Auditar cambios en el sistema a través de Kernel

Plan de Estudios



1. Seguridad en el Arranque

- Acceso Sin Contraseña
- Crear contraseñas para GRUB2
- Creación de Script de Configuración
- Prueba de Funcionamiento
- Política de Contraseñas
- Archivo /etc/shadow

2. IPTables

- Estructura de IPTables
- El comando IPTables
- Listar reglas
- Políticas por Defecto
- Agregar Reglas: Append vs Insert
- Eliminar Reglas: Por comando y por número

3. IPTables Avanzado

- Cadenas Personalizadas
- Creación de una cadena personalizada
- Desviando tráfico a una cadena personalizada
- El objetivo RETURN
- Listas de Filtrado con Cadenas Personalizadas
- IPSets

4. Detección de Intrusos

- IDS/IPS
- HIDS/HIPS vs NIDS/NIPS
- Monitoreo de Sistema de Archivos
- Samhain
- Instalación

Inicialización de la Base de Datos

5. MFA, Knockd, Auditd

Autenticación Multi-Factor (MFA)

Introducción

OTPW - Instalación

Configuración de PAM

Configuración de SSH

Creación de Contraseñas

EDUCACIÓN IT

Centro de Capacitación y Desarrollo Profesional



Lavalle 648 Piso 8, Microcentro, CABA

0810-220-8148

info@educacionit.com

EducaciónIT. Copyright 2005-2021