Seguridad en Linux: Server Hacking

Duración: 3 días (24 hrs)

Descripción general
Conoce las técnicas y herramientas que puedes utilizar para **garantizar la seguridad** de tu sistema operativo Linux. Define reglas de filtrado y domina la defensa y los ataques preventivos dentro de tus servidores.

Objetivos
- Definir políticas de seguridad para contraseñas y cuentas de usuarios
- Protección de datos confidenciales con cifrado de Volúmenes de Disco
- Cómo filtrar tráfico en base a protocolos, puertos y direcciones IP
- Mitigar ataques Dos/DDos con reglas IPTables
- Cómo identificar un malware oculto en el sistema
- Accesos físicos y remotos: protección de ataques y autenticación multi-factor
- Auditar cambios en el sistema a través de Kernel

Prerrequisitos del curso
Se requieren conocimientos sólidos en:
- Configuración, administración y mantenimiento de redes Linux o haber realizado el curso Linux Redes
- Seguridad en redes o haber realizado el curso Seguridad en Redes: Network Hacking

Esquema del curso

Linux y entornos virtuales

- Configuración de un entorno virtual Linux
- Introducción a RHEL (Red Hat Enterprise Linux)
- Introducción a Ubuntu
- Configuración de un Servidor Amazon Linux

Seguridad en Cuentas de Usuarios y Grupos

- Usuarios administrativos
- El grupo predefinido admin
- El archivo de políticas sudo
- Usuarios sudo limitados
- Prevención de ataques de fuerza bruta en contraseñas
- Bloquear de cuentas de usuarios

Seguridad del Servidor y el Firewall

- Introducción a iptables
- Zonas y servicios
- Introducción a nftables

Encriptación y Aseguramiento del SSH

- Encriptación de Particiones
- Encriptación de Directorios
- Encriptación de Volúmenes
- Aseguramiento de SSH (sustitución de contraseñas por archivos de claves)

Control de Acceso a Archivos y Directorios

- Autoria de archivos y directorios con `chown`
- Permisos de archivos y directorios con `chmod`

Listas de Control de Acceso

- Introducción a las ACL (Access Control Lists)
- Listas de acceso a usuarios y grupos
- Listas de acceso heredables en directorios
- Permisos específicos en la máscara del ACL
- Directorios compartidos

Control de Acceso con SELinux

- Introducción a SELinux
- Configuración de los contextos de seguridad
- Políticas de Seguridad de SELinux

Auditoría de Seguridad

- Introducción a ClamAV
- Auditoría de Archivos
- Auditoría de Directorios
- Auditoría de Llamadas del Sistema
- Búsquedas en cambios de archivos
- Búsquedas en cambios de directorios
- Búsquedas en reglas de violación de llamadas del sistema

Malwares, Vulnerabilidades y Detección de Intrusos

- Scaneo y uso de Lynis
- Búsqueda de vulnerabilidades con OpenVAS
- Escaneo del servidor web con Nikto

Protocolos Comúnes de Seguridad

- Audiroria de los servicios del sistema con `systemctl`
- Auditoria de los servicios de red con `netstat`
- Auditoria de los servicios de red con `nmap`
- Reseteo de la contraseña
- Prevención en la edición de parámetros del kernel