



PROFESSIONAL LINUX CONSULTING & TRAINING

CURSO DE SEGURIDAD LINUX

OBJETIVO

Que el estudiante entienda y aplique los sistemas, protocolos y procedimientos de seguridad y autenticación en servidores y estaciones de trabajo Linux



TEMARIO

SECCION I SEGURIDAD Y AUTENTICACION DE LA RED Y LOS SERVICIOS

- **Introducción a la seguridad**
 - Qué es la seguridad computacional
 - Controles de seguridad
- **Evaluación de vulnerabilidades**
 - Pensando como el enemigo
 - Evaluando y probando vulnerabilidades
 - Evaluando las herramientas
- **Atacantes y vulnerabilidades**
 - Historia breve de los hackers
 - Amenazas contra la seguridad de la red
 - Amenazas contra la seguridad los servidores
 - Amenazas contra la seguridad los usuarios
- **Ataques y exploits comunes**
- **Actualizaciones de seguridad**
 - Actualizando los paquetes
- **Asegurando el sistema**
 - Evaluando la seguridad del sistema
 - Seguridad del BIOS y el gestor de arranque
 - Seguridad de las contraseñas
 - Controles administrativos
 - Servicios de red disponibles
 - Firewalls personales
 - Herramientas de comunicación seguras
- **Asegurando los servidores**
 - Asegurando los servicios con TCP Wrappers y xinetd
 - Asegurando el servicio Portmap
 - Asegurando el servicio NIS
 - Asegurando el servicio NFS
 - Asegurando el servicio HTTP
 - Asegurando el servicio FTP
 - Asegurando el servicio SMTP



- Verificando los puertos abiertos
- **Entendiendo el funcionamiento de Pluggable Authentication Modules (PAM)**
 - Ventajas de PAM
 - Archivos de configuración PAM
 - Formato de los archivos de configuración PAM
 - Ejemplos de Archivos de configuración PAM
 - Creando módulos PAM
 - Caché de credenciales y PAM
 - Pertenencia de dispositivos y PAM
- Entendiendo el funcionamiento de TCP Wrappers y xinetd
 - TCP Wrappers
 - Archivos de configuración de TCP Wrappers
 - xinetd
 - Archivos de configuración de xinetd
- **Implementando la autenticación con Kerberos**
 - Qué es Kerberos
 - Terminología Kerberos
 - Cómo funciona Kerberos
 - Kerberos y PAM
 - Configurando el servidor Kerberos
 - Configurando el cliente Kerberos
 - Mapeando Dominios DNS-Kerberos
 - Configurando servidores secundarios
 - Configurando autenticación entre dominios

- **Implementando Redes Privadas Virtuales (VPN)**
 - Cómo funcionan las VPNs
 - Creando una conexión IPsec
 - Instalando Ipsec
 - Configurando IPsec Host-to-Host
 - Configurando Ipsec Network-to-Network
 - Iniciando y deteniendo una conexión Ipsec
- **Implementando un FireWall con IPTables**
 - Qué es NetFilter e IPTables
 - Configuración básica de un FireWall
 - Usando IPTables
 - Usando las reglas de FILTER
 - Usando las reglas de NAT y FORWARD
 - Software malicioso y direcciones IP falsificadas
 - Seguimiento de conexiones
 - IPV6
- **Trabajando con las opciones avanzadas de IPTables**
 - Filtrado de paquetes
 - Diferencias entre IPTables e IPChains
 - Opciones de comando de IPTables
 - Guardando las reglas de IPTables
 - Scripts de control de IPTables
 - IPTables e IPV6

SECCION II MECANISMOS DE SEGURIDAD CON SELINUX

- **Mecanismos de control de acceso (ACM)**
 - Control de Acceso
 - Discrecional (DAC)
 - Listas de Control de Acceso (ACL)



- Control de Acceso Obligatorio (MAC)
- Control de Acceso Basado en Roles (RBAC)
- Seguridad MultiNivel (MLS)
- Seguridad MultiCategoría (MCS)
- **Introducción a SELinux**
 - Panorama de SELinux
 - Archivos relacionados con SELinux
- **Antecedentes e historia de SELinux**
- **Seguridad MultiCategoría (MCS)**
 - Introducción
 - Aplicaciones para la Seguridad MultiCategoría (MCS)
 - Contextos de seguridad de SELinux
- **Comenzando con la Seguridad MultiCategoría (MCS)**
 - Introducción
 - Comparando SELinux y las Identidades de los Usuarios
 - Configurando Categorías
 - Asignando Categorías a los Usuarios
 - Asignando Categorías a los Archivos
- **Seguridad MultiNivel (MLS)**
 - Por qué MultiNivel
 - Niveles de Seguridad, Objetos y Sujetos
 - Políticas de MLS
- **Panorama de Políticas de SELinux**
 - Qué son las Políticas de SELinux
 - Dónde están las Políticas
 - El rol de las Políticas en el proceso de arranque
 - Clases de Objetos y Permisos
- **Panorama de las Políticas Dirigidas**
 - Qué son las Políticas Dirigidas
 - Archivos y directorios de las Políticas Dirigidas
 - Entendiendo el rol de los usuarios en las Políticas Dirigidas
- **Implementando el Control de Usuarios con SELinux**
 - Moviendo y copiando archivos
 - Checando el Contexto de Seguridad de un Proceso, Usuario o Archivo
 - Reetiquetando un archivo o directorio
 - Creando archivos que mantengan Contextos de Seguridad
- **Administrando SELinux**
 - Viendo el estatus de SELinux
 - Reetiquetando un sistema de archivos
 - Administrando directorios de usuario en NFS
 - Otorgando acceso a un directorio o árbol de



- directorios
- Respaldando y restaurando el sistema
- Habilitando y deshabilitando la aplicación de las Políticas
- Habilitando y deshabilitando SELinux
- Cambiando las Políticas
- Especificando el Contexto de Seguridad de sistemas de archivos
- Cambiando la Categoría de Seguridad de un archivo o usuario
- Corriendo un comando en un Contexto de Seguridad específico
- Comandos útiles para

scripts

- Cambiando a un Rol diferente
- Cuando reiniciar
- **Analizando el comportamiento SELinux**
 - Habilitando auditorías en el kernel
 - Viendo los archivos de historiales
- **Configurando las Políticas de SELinux**
 - Introducción a las Políticas modulares
 - Construyendo un módulo de Políticas Locales

Duración: 25 horas

Material: CD de Red Hat Linux

Documentación: Manuales Oficiales de Red Hat Linux

