



DIPLOMADO

ADMINISTRADOR DE REDES LINUX

CON ORIENTACIÓN EN CIBERSEGURIDAD Y ETHICAL HACKING CON KALI LINUX

RESOLUCIÓN 118/25

Certificación UTN-FRD



TEMARIO DEL CURSO

Administrador de Redes Linux

CLASE 1

Introducción

- ▶ Conceptos básicos.
- ▶ Historia. El proyecto GNU.
- ▶ El software libre. Kernel Linux. Tipos de licencias.
- ▶ Distribuciones GNU/Linux.
- ▶ Instalación del sistema operativo.

CLASE 2

Instalación del Sistema Operativo

- ▶ Particiones.
- ▶ El FHS (Filesystem Hierarchy Standard).

CLASE 3

Proceso de Login y Primeros Comandos

- ▶ La secuencia de arranque
- ▶ SystemV o SysVinit.
- ▶ Upstart.
- ▶ Inicio del sistema. Systemd.
- ▶ El proceso de login.
- ▶ El modo texto. Los primeros comandos.

CLASE 4

Comandos GNU/Linux

- ▶ Moviéndonos por el sistema de Archivos.
- ▶ Crear directorios y árboles de directorios.
- ▶ Crear archivos con touch.
- ▶ Borrar directorios y archivos.
- ▶ Copiar archivos y directorios.
- ▶ Mover archivos y directorios.
- ▶ El comando ln. Apagar y reiniciar el sistema.

CLASE 5

Manejo de Archivos

- ▶ Uso de cat y zcat.
- ▶ Uso de less y zless.
- ▶ Man pages (manuales).
- ▶ Uso de head y tail.
- ▶ Contar líneas, palabras, y caracteres con wc.
- ▶ Uso de diff.
- ▶ Búsquedas básicas y avanzadas.

CLASE 6

Editor de Textos VI

- ▶ Modos de operación.
- ▶ Desplazamiento.
- ▶ Copiar, pegar y cortar.
- ▶ Repeticiones de comandos.
- ▶ Insertar contenido externo.
- ▶ Comparativa con el editor de textos nano.

CLASE 7

Administración de Dispositivos de Almacenamiento

- ▶ Los sistemas de archivos.
- ▶ Crear particiones y sistemas de archivos.
- ▶ Montar particiones.
- ▶ El archivo /etc/fstab.

CLASE 8

Administración de Procesos

- ▶ Concepto y clasificación de procesos.
- ▶ Uso de pstree.
- ▶ El comando ps.
- ▶ Los comandos kill y killall.
- ▶ Concepto de señales.
- ▶ Uso de top.
- ▶ Administración de servicios.

CLASE 9

Administración de Usuarios y Permisos

- ▶ Introducción a la administración de usuarios.
- ▶ Crear usuarios y grupos.
- ▶ Administración de grupos.
- ▶ Permisos en Linux.
- ▶ Permisos especiales y ACL

CLASE 10

Administración de Paquetes

- ▶ Uso de dpkg en Debian y derivados.
- ▶ Uso de apt-cache y apt-get en Debian y derivados.
- ▶ Uso de RPM en Centos y similares.
- ▶ Uso de Yum en Centos y similares.
- ▶ Familia SUSE. Uso de zypper.

CLASE 11

RAID

- ▶ Niveles (tipos) más utilizados.
- ▶ Crear RAID por software.
- ▶ Administración de RAID.

CLASE 12

LVM (Logical Volume Management)

- ▶ Creación de volúmenes físicos.
- ▶ Grupos de volúmenes.
- ▶ Volúmenes lógicos.

CLASE 13

Shell Scripting

- ▶ Configurar el entorno de la shell.
- ▶ Ejecución encadenada de comandos.
- ▶ Uso de condicionales.
- ▶ Bucles.
- ▶ La estructura Case.

CLASE 14

Syslog y Tareas Programadas

- ▶ Cron.
- ▶ Cron y Anacron.
- ▶ Los Timers en Systemd.
- ▶ Uso de at.
- ▶ El archivo rsyslog.conf
- ▶ Uso de logger.
- ▶ Registro de eventos con journald.

CLASE 15

Quotas de Disco

- ▶ Bloques e ínodos.
- ▶ Opciones de montaje.
- ▶ Activar y editar cuotas.
- ▶ Período de gracia.
- ▶ Reportes y avisos de cuotas excedidas.

CLASE 16

Conceptos Fundamentales sobre Redes

- ▶ Protocolos.
- ▶ Paquetes de red.
- ▶ TCP/IP.
- ▶ Servicios de red.
- ▶ Comprobaciones con traceroute.
- ▶ Uso de ifconfig y route.
- ▶ El grupo de herramientas ip.
- ▶ Los comandos host y dig.
- ▶ Netstat y ss.

CLASE 17

Configuración de DHCP

- ▶ Preparación del cliente y del servidor.
- ▶ Configuración del servidor.
- ▶ Verificación del cliente.
- ▶ Otorgar una dirección de un rango disponible.

CLASE 18

Configuración de DNS

- ▶ El archivo /etc/hosts.
- ▶ Resolución de nombres paso a paso.
- ▶ El archivo /etc/resolv.conf.
- ▶ Configuración de bind.
- ▶ Configuración de zonas (directa e inversa).
- ▶ Uso de dig para hacer consultas a servidores DNS.

CLASE 19

Configuración de SSH

- ▶ Conexión a través de ssh.
- ▶ Configuración del servidor ssh.
- ▶ Uso de scp, sftp, ssh-agent, y ssh-add.

CLASE 20

Configuración de FTP

- ▶ Introducción a file transfer protocol.
- ▶ Configuración de vsftpd.
- ▶ Modos FTP.

CLASE 21

Configuración de NFS

- ▶ Introducción a network file system.
- ▶ El archivo /etc/exports.
- ▶ El comando exportfs.
- ▶ Autofs.

CLASE 22

Configuración de Samba

- ▶ El servidor Samba.
- ▶ Cliente Samba.

CLASE 23

Apache Web Server

- ▶ Directorio principal de configuración.
- ▶ El archivo apache2.conf.
- ▶ Logs de acceso y error.
- ▶ Hosts virtuales. Implementación de https para un host virtual.

CLASE 24

SQUID e IPTABLES

- ▶ Introducción a iptables.
- ▶ Firewall con iptables.
- ▶ Squid. Configuración básica.

TEMARIO DEL CURSO

Ciberseguridad

CLASE 1

Introducción al Ethical Hacking

- ▶ ¿Qué es el “ethical hacking”?
- ▶ Valores fundamentales.
- ▶ Objetivos de la seguridad informática.
- ▶ Análisis de riesgos.
- ▶ Puesta en marcha de una política de seguridad.

CLASE 2

Footprinting

- ▶ ¿Qué saben los buscadores de nuestro objetivo?
- ▶ Servicios Web de búsqueda de información de un dominio.
- ▶ Obtener información de los DNS.
- ▶ Fuzzing web.

CLASE 3

System Hacking

- ▶ Windows System Hacking.
- ▶ Contramedidas.
- ▶ Linux System Hacking.

CLASE 4

Scanning & Enumeration

- ▶ Funcionamiento de Nmap.
- ▶ Como usar Nmap.

CLASE 5

SQL Injection

- ▶ Trabajando con SQL Injection.

CLASE 6

Web Application Vulnerabilities

- ▶ Vulnerabilidades en aplicaciones web.
- ▶ Funcionamiento de w3af.
- ▶ Vulnerabilidades OS Command.

CLASE 7

Honeypots

- ▶ ¿Qué es un honeypot?
- ▶ Clasificación de honeypots.
- ▶ Honeypots en producción.
- ▶ Honeypots en desarrollo.

CLASE 8

Linux Hacking

- ▶ ¿Por qué atacar sistemas Linux?
- ▶ Scanlogd. Abacus Portsentry.
- ▶ Sniffit. John the Ripper.

CLASE 9

Criptografía

- ▶ ¿Cómo es el proceso de criptografía simétrica?
- ▶ ¿Cómo es el proceso de criptografía asimétrica?
- ▶ Introducción a firma digital.
- ▶ GPG (Gnu Privacy Guard).

CLASE 10

Criptografía II

- ▶ Criptografía y seguridad en computadores.

CLASE 11

Virus, Troyanos y Backdoors

- ▶ Virus informáticos y sistemas operativos.
- ▶ Métodos de propagación
- ▶ Métodos de protección y tipos
- ▶ Troyanos Backdoor de acceso remoto, Planificación.

CLASE 12

Hacking Wireless Networks

- ▶ Redes Inalámbricas. Suite “aircrack-ng”.
- ▶ WEP (Wired Equivalent Privacy). WPA (Wi-Fi Protected Access).
- ▶ PSK (Phase Shift Keying). TKIP (Temporal Key Integrity Protocol).
- ▶ AES (Advanced Encryption Standard).

CLASE 13

IDS Evasion

- ▶ Evasión de firewalls
- ▶ Evasión de IDS.

CLASE 14

Host Intrusion Detection System

- ▶ HIDS: Host Intrusion Detection System

CLASE 15

Network IDS

- ▶ NIDS: Network Intrusion Detection System.
- ▶ SNORT.
- ▶ Modos de ejecución.

CLASE 16

Tripwire

- ▶ Instalación
- ▶ Iniciando tripwire.

CLASE 17

Ingeniería Social

- ▶ Phishing.
- ▶ Técnicas de phishing.
- ▶ Variantes.

CLASE 18

Buffer Overflow

- ▶ Buffer overflow.
- ▶ Desarrollo de un exploit.

CLASE 19

Session Hijacking

- ▶ Hijacking.
- ▶ ¿Qué es el secuestro de sesiones?
- ▶ Pasos para secuestrar una sesión web.

CLASE 20

Sniffers

- ▶ ¿Qué es un snifer?
- ▶ ¿Cómo trabaja un snifer?
- ▶ ¿Cómo ocultar su presencia?
- ▶ Instalar un snifer en modo no promiscuo.

CLASE 21

Sniffers II

- ▶ Prácticas de sniffing.

CLASE 22

Pentesting y Metasploit

- ▶ Definición de pentesting.
- ▶ Normas y certificación.
- ▶ Tipos de prueba.
- ▶ Distribuciones de sistemas operativos especializados.

CLASE 23

DOS

- ▶ Denegación de servicios.
- ▶ Métodos de ataque.

CLASE 24

Web Server Security

- ▶ Hacking Web Servers.
- ▶ Ataques más comunes a los servidores web.
- ▶ Cómo incrementar la seguridad en servidores web.
- ▶ Herramientas para atacar servidores web.

TEMARIO DEL CURSO

Hacking Ético con Kali Linux

CLASE 1

- ▶ Introducción a la seguridad informática
- ▶ Seguridad de la información □ Modelo PDCA
- ▶ Bases de la seguridad informática
- ▶ Mecanismos básicos de seguridad
- ▶ Vulnerabilidades de un sistema informático
- ▶ Políticas de seguridad
- ▶ Amenazas
- ▶ Hacktivismo
- ▶ Clases de hackers
- ▶ Clases de hackers éticos
- ▶ Perfil de habilidades de un hacker ético
- ▶ La evaluación de seguridad
- ▶ Qué se debe entregar en los test de hacking ético

CLASE 2

- ▶ Prevención y detección de malware
- ▶ Introducción al malware
- ▶ Historia del malware □ Evolución e hitos
- ▶ Tipos de malware □
- ▶ Virus
- ▶ Gusano
- ▶ Troyano
- ▶ Adware
- ▶ Spyware
- ▶ Ransomware
- ▶ Rootkit

CLASE 3

- ▶ Instalación de Kali Linux
- ▶ Métodos de Instalación
- ▶ Crear un USB booteable con Kali Linux
- ▶ Crear un USB persistente con Kali Linux

CLASE 4

- ▶ Virtualización de Kali Linux
- ▶ Instalación de Kali Linux en maquinas virtuales
- ▶ Cómo se importa nuestro kali linux
- ▶ Cómo armar un laboratorio básico para hacking ético

CLASE 5

- ▶ Introducción a GNU/Linux
- ▶ Distribuciones de pentesting y forensia.
- ▶ Política de actualizaciones. Apt.
- ▶ Gestión de códigos fuentes (tarball).
- ▶ Administración de archivos de configuración. Etc.

CLASE 6

- ▶ Reconocimiento pasivo
- ▶ Información de dominios. Whois.
- ▶ OSINT – Obtener correos, números y nombres
- ▶ Shodan
- ▶ Encontrar versiones anteriores de páginas web
- ▶ Encontrar ubicaciones por medio de metadatos
- ▶ Entrar a cámaras de seguridad
- ▶ Rastreo de IP
- ▶ Confidencialidad, integridad y disponibilidad de la información

CLASE 7

- ▶ Introducción al footprinting
- ▶ Footprinting activo
- ▶ Maltego
- ▶ Shodan
- ▶ Fingerprinting

CLASE 8

- ▶ Reconocimiento activo
- ▶ Rastreo de puertos abiertos
- ▶ Nmap
- ▶ Scripts de nmap
- ▶ OSINT + reconocimiento activo

CLASE 9

- ▶ Análisis de vulnerabilidades.
- ▶ Introducción al análisis de vulnerabilidades
- ▶ Instalación de Nessus Essentials
- ▶ CVEs y CWEs
- ▶ OWASP

CLASE 10

- ▶ Explotación
- ▶ Metasploit framework
- ▶ Armitage.
- ▶ Msfvenom. Infectando aplicaciones Android.
- ▶ Explotación de vulnerabilidades

CLASE 11

- ▶ Ejemplos prácticos de Post-Explotación
- ▶ Persistencia
- ▶ Pivoteo
- ▶ Robo de credenciales
- ▶ Descarga de archivos
- ▶ Post-Reconocimiento local
- ▶ Dirección IP

CLASE 12

- ▶ Controlando el sistema remotamente
- ▶ Información del sistema e interfaces de red
- ▶ Shell y Meterpreter
- ▶ Manejo de archivos y procesos.
- ▶ Capturas de pantalla. Keylogger. Capturas cámara web y micrófono.

CLASE 13

- ▶ Auditoría wireless
- ▶ Suite aircrack-ng en la auditoría de contraseñas de redes wifi
- ▶ Uso de macchanger y su rol en la desautenticación
- ▶ Airodump-ng y la captura de paquetes
- ▶ Aireplay-ng y los ataques más comunes de inject frames
- ▶ Airgeddon como herramienta script para la automatización de AW

CLASE 14

- ▶ Enumeración
- ▶ ¿Qué es la enumeración?
- ▶ Técnicas para la enumeración
- ▶ Sesiones nulas
- ▶ Enumeración de netbios
- ▶ Contramedidas
- ▶ Enumeración ntp y smtp

CLASE 15

- ▶ Craqueo de contraseñas
- ▶ Ataques a las contraseñas
- ▶ Tipos de contraseñas
- ▶ Ataque en línea pasivo y activo
- ▶ Ataques fuera de línea
- ▶ Ataque en red distribuido
- ▶ Ataque por tablas de arcoíris
- ▶ Contramedidas y mitigación de vulnerabilidades en las contraseñas

CLASE 16

- ▶ Administración de usuarios
- ▶ Manejo de usuarios
- ▶ Importancia del usuario root
- ▶ El sistema de permisos de GNU/Linux
- ▶ Control de acceso
- ▶ Manejo de procesos. Top. Ps ax.
- ▶ Contramedidas de Seguridad en la Lista de Control de Acceso (ACL's)

CLASE 17

- ▶ Escalada de privilegios
- ▶ Métodos de ataque para escalar privilegios
- ▶ Ataques desde copias de seguridad de la SAM
- ▶ Extracción de hashes
- ▶ Herramientas

CLASE 18

- ▶ Cubrir las huellas
- ▶ Etapa 5 cubriendo el rastro
- ▶ Detener las auditorias del sistema
- ▶ Borrar los eventos
- ▶ Borrar logs remotamente

CLASE 19

- ▶ Formas de ocultar información
- ▶ Criptografía
- ▶ Encriptación en archivos
- ▶ Cifrado punta-punta

CLASE 20

- ▶ Esteganografía y estegoanálisis
- ▶ Introducción y conceptos
- ▶ Herramientas
- ▶ Esteganografía en archivos de texto y en imágenes
- ▶ Esteganografía en archivos de audio. Concatenando archivos.
- ▶ Actividades básicas de estegoanálisis

CLASE 21

- ▶ Sniffing
- ▶ Uso básico de Wireshark
- ▶ Defensa ante técnicas de sniffing
- ▶ Filtros
- ▶ Análisis de paquetes
- ▶ Captura de contraseñas, a través de la interceptación de tráfico

CLASE 22

- ▶ Social Engineering práctico
- ▶ Uso de SET en Kali Linux
- ▶ Beef project como herramienta de ingeniería social

CLASE 23

- ▶ El proyecto TOR
- ▶ Privoxy
- ▶ Proxychains
- ▶ Anonimato en la web
- ▶ Deep web y Dark Web

CLASE 24

- ▶ Forensia
- ▶ Análisis forense
- ▶ Recuperación de archivos borrados
- ▶ Recuperación de partición eliminadas
- ▶ Autopsy. Análisis de metadata de archivos
- ▶ Análisis de memoria. Volatility.
- ▶ Adquisición forense