

Master in Cybersecurity and Ethical Hacking



Este entrenamiento es perfecto para aquellos profesionales que quieran incursionar en la **Ciberseguridad** y **Hacking Ético** de Tecnologías de TI e Internet, donde se examinarán técnicas de **Hardening**, **Pentesting**, **Navegación en la Red profunda** (Deep Web), **Análisis de tráfico**, **Firewall/VPNs**, **XSS Web**, **Seguridad Wireless**, **Google Hacking**, **SQL Injection**, **Hacking con inteligencia artificial (IA)** y medidas de prevención utilizando herramientas avanzadas de seguridad y de **Clase mundial**.



“ Este entrenamiento se lleva a cabo en un laboratorio extremadamente desafiante utilizando escenarios reales que enfrentan los profesionales en **Offensive Security** durante las pruebas de penetración en vivo y estarás listo para aprobar el examen de Certificación **Ethical Hacking Professional Certification (CEHPC)**. ”



DIRIGIDO A:

Pentesters, Hackers Éticos, Investigadores, Auditores de Ciberseguridad, Especialistas en TI, Proveedores de Internet y profesionales deseen actualizar sus conocimientos en Ciberseguridad.

REQUISITOS:

- Conocimientos básicos de **Networking TCP/IP, Linux y Windows**

Que voy aprender..

- 1. Conceptos clave en ciberseguridad.** Comprenderás aspectos e importancia de la seguridad de la información y la seguridad de la red
- 2. Hardening en servidores Linux/Unix.** Aprenderás a Blindar servidores, intranets y servicios
- 3. Amenazas, vulnerabilidades y ataques a la seguridad de la información**
- 4. Malware.** Conocerás diferentes tipos de código malicioso y como mitigarlo
- 5. La Deep Web y la Dark Net.** Conocerás sus riesgos y navegara en la red Oscura
- 6. Comprenderás técnicas de ataque de Ingeniería social y Ciber-inteligencia**
- 7. Comprender ataque de denegación de Servicios.** Comprenderás que es un ataque DoS/DDoS y como mitigarlos
- 8. Técnicas y herramientas de evaluación de la seguridad de la red** (búsqueda de amenazas, inteligencia de amenazas y vulnerabilidades
- 9. Hacking Ético.** Aprenderás la metodología de pruebas de penetración
- 10. Ataques servidores Web y Bases de datos.** Realizaras ataques XSS, CSRF, SQL Injection y como evitarlos

Que voy aprender..

- 11. Hacking Ético.** Aprenderás la metodología de pruebas de penetración en tus activos informáticos
- 12. Ataques a redes inalámbricas (Wireless) WEP, WPA/WPA2 PSK y como evitarlos**
- 13. Utilizaras Inteligencia Artificial (IA) para Hacking Ético.** Aprenderás a usar estas nuevas herramienta para el **Hacking**
- 14. Realizar ataques a dispositivos móviles (Google Android) y su mitigación**
- 15. Fundamentos de dispositivos móviles, IoT y OT y medidas de seguridad relacionadas**
- 16. Criptografía e infraestructura de clave pública**
- 17. Implementaras seguridad perimetral.** Configuraras **Firewalls, VPNs y DMZ**

MÓDULOS:

Hardening en Servidores Linux/Unix

MODULO

01



En este módulo se ve el **Hardening** de servidores **Linux/Unix**, a través de configuraciones y estándares de seguridad, así como la instalación del software necesario. También incluiremos consejos sobre mejores prácticas de registro, auditoría y cumplimiento. Todo esto ayuda con la detección temprana en caso de que sus servidores se vean comprometidos.

Requisitos: Conocimientos de **Linux** y redes **TCP/IP**.

Duración: 16 hrs.

01

Gestión de Seguridad de la Información ISO/IEC 27001:2022

- Introducción a la seguridad de la información
- Conceptos y definiciones de la Norma **ISO 27001:2022**.
- Gestión de la seguridad de la información, para proteger a una organización de las amenazas internas y externas
- Objetivos de la seguridad en **TI**: **Confidencialidad, Disponibilidad, Integridad, No repudio**
- Estructura y gobierno de la seguridad de la información
- Riesgos y estrategias de la seguridad de la información
- Eventos incidentes y dominios de control
- Pruebas, sensibilización y evaluación de **SGSI**

02

Marco de ciberseguridad del NIST

- Estándares de ciberseguridad aceptados: **NIST SP 800-53, COBIT 5 ISO/IEC 27001:2022 y CIS CSC**.
- Estructura central del marco de ciberseguridad del **NIST**
- Niveles de implementación del marco **NIST**
- Establecimiento de un programa de gestión de riesgos de ciberseguridad del marco **NIST**

Hardening en Servidores Linux/Unix

03

Hardening (Blindaje) a Servidores Linux/Unix

- Instalación segura de servidores **Linux/Unix**
- Estándares de seguridad básicos para **S.O** de red
- Instalación segura, particiones y seguridad
- Particiones primarias, extendidas y lógicas
- Sistema **RAID (Redundant Array of Inexpensive Disks)**
- Hardware **RAID** vs. Software **RAID**
- Elección del método de arranque
- Implementación de Sistemas **RAID**
- Creación de **LVM (Logical Volume Management)** paso a paso

04

Hardening al sistema operativo

- Explicación de los archivos **/etc/passwd /etc/group /etc/shadow**
- Gestión de usuarios y grupos
- Comandos para cambiar la propiedad de un elemento: **chgrp** y **chown**
- Cambio de permisos de archivos y directorios en **Linux/Unix** con **chmod**
- Cambiar permisos con **chmod** en modo octal (números)
- Permisos especiales de **Linux**: **setUID**, **setGID** y **Sticky bit**
- Prácticas con permisos especiales de **Linux**
- Listas de Control de Acceso (**ACL**)
- Los atributos del sistema de ficheros de Linux: **lsattr** y **chattr**
- Seguridad en los privilegios de usuario: **sudo** y **sudoers**
- Supervisar actividad de usuarios: **who**, **last** y **w**

05

Seguridad básica

- Establecer la complejidad de las contraseñas de **login** en **Linux**
- Bloqueo a usuarios con intentos de acceso fallidos
- Configuración de bloqueador de ataques de fuerza bruta
- Encontrar posibles riesgos en el uso del sistema de ficheros
- permisos peligrosos en el sistema de ficheros.
- supervisar el uso de ficheros con **lsof** y **fuser**
- Monitoreo de disco: comandos **du** y **df**
- Comandos para supervisar y administrar procesos **Linux**
- Controlar la carga del sistema. Uso de memoria y **cpu**

06

Habilitar SELinux

- Activar el mecanismo de control de acceso integrado **Security-Enhanced Linux (SELinux)**.

07

Política de contraseñas fuertes

- Las mejores prácticas para crear contraseñas
- Deshabilite las cuentas con contraseñas vacías
- Solicite a los usuarios que establezcan contraseñas seguras
- Deshabilitar la cuenta root
- Uso de sudo, para una mejor auditoría y control.
- Técnicas para generar contraseñas más seguras y más difíciles adivinar

08 Eliminar paquetes innecesarios

- enumere todos los paquetes y el software instalado en sus servidores utilizando sus administradores de paquetes (**apt**, **yum**, **dpkg**).
- desinstalar programas innecesarios.

09 Kernel y Paquetes actualizados

- paquetes actualizados con las últimas actualizaciones de seguridad para evitar la explotación de vulnerabilidades conocidas.

10 Hardening a Networking

- Deshabilitar **ICMP**
- explotar **ICMP** para obtener información sobre las redes atacadas
- ataques maliciosos que incluyen descubrimiento de red
- canales de comunicación encubiertos y redirecciones de tráfico de red.
- **Ping sweep**.- los atacantes usan esto para identificar todos los hosts en una red.
- **Ping flood**.- los atacantes pueden enviar mensajes **ICMP** en rápida sucesión, provocando el agotamiento del ancho de banda entrante y saliente.

11 Deshabilitar IPv6

- Si no utilizan el protocolo **IPv6**
- Desactivación desde **/etc/sysconfig/network**

12 Secure Shell Protocol

- Configuración de **IPTables** y el acceso **SSH** desde IP conocidas
- Autenticación basada en claves
- Configuración del servidor y inicio de sesión **root**

13 Cierre de puertos innecesarios

- Uso de **netstat** para escuchar conexiones entrantes
- Desactivación y eliminación de conexiones entrantes sospechosas
- Bloqueo de puertos no utilizados

14 Configuración del Firewall

- Uso de **Linux iptables** para el control **incoming**, **outgoing** y **forwarded** para proteger servidores
- Configuración de reglas para permitir y denegar tráfico desde IP específicas

15 Registro y auditoría

- Registro y la auditoría detallados habilitados para sus servidores
- Detección de intentos de intrusión.
- Medición del alcance de la violación e información para una autopsia
- **Syslog** y el directorio **/var/log**
- Funcionamiento del demonio **rsyslog**
- Práctica: configuración de **rsyslog**
- Uso de **journalctl** para filtrar mensajes del sistema

16 Cierre de puertos innecesarios

- Uso de **netstat** para escuchar conexiones entrantes
- Desactivación y eliminación de conexiones entrantes sospechosas
- Bloqueo de puertos no utilizados

17

Copias de seguridad periódicas

- Configuración de copias de seguridad de datos

18

Monitoreo de amenazas y cumplimiento

- Estas herramientas monitorean constantemente toda su infraestructura, identificando y deteniendo códigos maliciosos o no autorizados cuando intentan ejecutarse.

Pentesting y Hacking Ético

MODULO

02



En este modulo aprenderás metodologías de **hacking ético**, **pruebas de penetración** Navegación en la Red profunda (**Deep Web**), Análisis de tráfico, **Ataques de día Zero** (**Zero-Day Attack**), **Dos/DDoS**, Análisis de **Malware**, **XSS Web**, Seguridad **Wireless**, **Google Hacking**, **SQL Injection**, **Hacking con inteligencia artificial (IA)**, ataque a Dispositivos Móviles (**Google Android®**) y Ingeniería Social, **Ciber-inteligencia**, medidas de prevención utilizando herramientas avanzadas de seguridad y de Clase mundial.

Requisitos: Conocimientos de **Linux/Windows** y redes **TCP/IP**.

Duración: 40 hrs.

1

Fundamentos de Cybersecurity

- Conceptos de Ciberseguridad
- **FootPrinting, FingerPrinting**
- Metadatos
- Recopilación de información
- Herramientas de recopilación de información
- **Whois, Ping, Traceroute**
- **Nslookup, dig, host**
- Metadatos, **Google Dorks**
- **Maltego, The Harvester, Dmitry**

2

La Deep Web y la Dark Web

- La Internet profunda
- Cómo acceder a la **Web Oscura**
- Hackers, miembros de las fuerzas del orden y criminales
- El navegador de red Tor (Proyecto “**The Onion Routing**”)
- ¿Es ilegal entrar en la web oscura?
- Anonimato del usuario
- Servicios y sitios prácticamente imposibles de rastrear
- Tipos de amenazas en la Web oscura

Laboratorio:

- Navegando por la **Deep Web**

3

Evaluación de vulnerabilidades

- Escaneo de puertos para realizar ataques
- Test de puertos abiertos
- Técnicas de escaneo de puertos
- **TCP Connect** , **TCP SYN**, **Stealth**, (**FIN Scan**), **ACK Scan**, **Null Scan**, **TCP Xmas Scan**, **Idle Scan**, **UDP ICMP Port Scan**, **ICMP ping-sweeping**
- **Nmap**, **Nmap Scripting**
- **CVE**, **CWE**, **CVSS**, **Nessus**, **OpenVas**
- Gestión de Vulnerabilidades
- Enumeración de recursos compartidos de red, usuarios y grupos, versiones de aplicaciones/servicios, transferencia de zona, Configuraciones, etc.

4

Explotación de Sistemas

- Manejo de **Exploits**
- Escalamiento de Privilegios
- Obtención de Credenciales
- Movimientos Laterales
- Explotación de sistemas
- **CrackMap**, **Powershell** para **pentesters**
- Rutas de explotación **Bloodhound**, Evasión de Defensas, **LoLbins**
- **Kerberoasting**, Algoritmos Criptográficos

5

Password Cracking

- Ataque basado en diccionario, fuerza bruta y basado en reglas
- Ataque a contraseña mediante técnica hombre en medio (**Man-in-the-Middle**)
- Ataque a contraseña mediante Troyanos, **Spyware** y **Keyloggers**
- Ataque a través de **Rainbow Tables** mediante valor **hash**
- **Crack** de algoritmos de cifrado: **MD5**, **SHA** y **Blowfish**
- **Crack** de contraseñas con **John the Ripper**

6

Explotación Avanzada con Metasploit Framework

- Línea de comandos de **Metasploit**
- **Metasploit** y sus componentes: **msfconsole**, **msfcli**, **msfgui**, **msfweb**, **msfpayload**, **msfencode**, **msfvenom**
- Etapas de un **Pentesting** y las herramientas en **Metasploit**
- Post-Explotación, ya tengo **shell** ... ¿ahora que hago?
- Trabajando con **Meterpreter**
- Ataques a máquinas **Windows** con **Metasploit**
- Ataque a servidores **FTP** con **Metasploit**
- Ataques a Android con **Metasploit**

7

Ataque a la red Interna en profundidad

- **Ataque a la red Interna en profundidad**
- Introducción al **ARP Spoofing**
- Mitigación de ataques **ARP Spoofing**
- Laboratorio: Realizar ataque **ARP Spoofing** con **Linux**
- Cómo protegerse de ataques **ARP Spoofing** con **ARPoN**
- Ataques **redirect** y **DHCP Spoofing**

8

Secuestro de sesiones

- **Hijacking** (secuestro de sesiones)
- Ataques **Man-in-the-middle**
- Cross-site scripting (**XSS**)
- Secuestro del lado de la sesión
- Fijación de sesión
- Contramedidas

9

Ingeniería Social y Cyberintelligence

- **Open Source Intelligence, Social Engineering**
- **Spear Phishing, USB Weaponization, Email Spoofing**
- **Psicología oscura**, ataque a comportamientos vulnerables
- Técnicas de ingeniería social utilizado **Malware** por los ciberdelincuentes

Explotación de Vulnerabilidades Web y SQL Injection

- Modelado de Amenazas
- Ataque y defensa a servidores **Web**
- Vulnerabilidades del servidor **Web** y manipulación de **URL**
- Aprovechamiento de las debilidades de sistemas de autenticación
- Vulnerabilidades en **XSS**
- Inyección de scripts maliciosos **Cross-site Scripting (XSS)**
- **XSS Reflejado**, **XSS Almacenado**, **XSS DOM**
- Como evadir el filtro para **XSS (Bypass XSS)**
- Vulnerabilidades en **LFI/RFI**
- **LFI/RFI** explotándolo y generando una **Shell**
- **OWASP (Open Web Application Security Project)**
- Cómo funciona **SQL Injection**
- Tipos de inyecciones **SQL**
- Métodos de envío de información
- Saltando la Seguridad en **Login**
- Buscando sitios vulnerables **GHDB**
- Detectando inyecciones por método **GET** y **POST**
- Herramientas de explotación
- Servidor para pruebas de caja negra: **DVWA**
- Identificando una **SQLi** con **DVWA**
- Inyección **SQL** utilizando **Union Select**
- Extraemos datos insertando sentencias **Union Select**
- Conocimientos Avanzados **SQLi** (Explotación)

11

Análisis y Monitoreo de Amenazas

- Análisis de **Malware**
- Análisis Estático, Análisis Dinámico
- **Sandboxing, Threat Intelligence**
- **ATT&CK Matrix**

12

Defensas contra Ciberataques

- **Asset Managment, Patch Managment, Threat Intelligence,**
- **Windows Hardening, CIS Benchmarks, HIDS, OSQuery, Logs.**
- Sistema de detección de intrusos (**IDS**)
- Arquitectura de un **IDS**
- Configuración **Firewall (IPTABLES)** e **IDS (SNORT)**
- **Snort** en modo **Sniffer**, y Detección de intrusos

13

Ataques a dispositivos de telefonía móvil

- Entender la estructura de Android y **APKs**
- Conceptos básicos sobre el sistema operativo **Android®**
- Crear **APKs** maliciosas
- Tomar control total de un Dispositivo Android
- Realizar ataques usando la cámara, geolocalización y usar herramientas de post explotación de **Metasploit**

14

Modelamiento de amenazas con Mitre ATT&CK®

- ¿Qué es el **Mitre ATT&CK®**?
- Panoramas adversos desde **Internet**
- Enfoque de amenazas basado en **Mitre ATT&CK®**
- Ciberataque, deben tomar un enfoque basado en el comportamiento del adversario (**IOA**)
- ¿Cuántas tácticas o etapas contiene el **Framework** de **Mitre ATT&CK®**?
- ¿A qué tecnologías se aplica **ATT&CK**?
- ¿Cómo puedo usar **ATT&CK**?
- Uso de **Attack Navigator**
- Uso de **Engage** y **Mitre CAR**

Laboratorio:

- Implementación de **LAB** con **Microsoft® Windows 11** y **Ubuntu**

15

Inteligencia artificial (IA) aplicado al Ethical hacking

- Inteligencia artificial orientada a la ciberseguridad
- Uso de: **ChatGPT**, **SecGPT**
- La **IA** orientada a **pentester**
- La **IA** identificando patrones emergentes de ataques
- Desarrollo de técnicas de explotación customizadas con **IA**
- Innovación de metodologías ofensivas con **IA**

Laboratorio:

- Identificar vulnerabilidades potenciales con **IA**
- Explotación de patrones emergentes de ataque **con IA**
- Ejemplos prácticos

16

Ataques DoS (Denial of Service) y DDoS (Distributed Denial of Service)

- Tipos de ataque **DoS**
- Inundación **SYN (SYN Flood)**, **ICMP (ICMP Flood)**
- Ataque **Smurf**
- **Ping** de muerte o inundación **ICMP**
- Inundación **SYN**
- Estrategia de defensa en ataques **DoS/DDoS**

17

Hacking a Redes Wireless

- La familia de protocolos **IEEE 802.11**
- Wireless y la inseguridad inherente
- La seguridad actual en Wireless: **WEP**, **WPA**, **WPA2** y **WPA3**
- Debilidades del cifrado y **Cracking WEP**
- Ataque pasivo y ruptura por estadística y diccionario
- Ataque activo de reinyección **ARP**
- Ataque de fuerza bruta mediante diccionario
- Buscar el objetivo: punto de acceso + clientes conectados
- Ataque de **de-autenticación**, Capturando el **handshake**
- Diccionario de claves
- Ataque a **WPS** y **Fake AP**
- **Evil Twin** y suplantación de identidad de punto de acceso **MAC**
- Punto de acceso renegado e ilegítimo
- **Honeypot** y ataque **MIS Association**
- Ataques avanzados **Wireless**

Firewalls/VPNs y Seguridad Perimetral

MODULO 03



Este modulo aborda aspectos sobre el funcionamiento y configuración de un **Firewalls** y **Redes Privadas Virtuales (VPN)**, en **Linux**, así como aspectos de diseño, reglas, cadenas, enmascaramiento, reenvío de paquetes, **Zonas Desmilitarizadas (DMZ)**, Además, aspectos de **encapsulación** y **encriptación**, en la cual los paquetes de datos viajan a distintos puntos remotos por medio de un **túnel**.

Requisitos: Conocimientos básicos de redes, **Linux/Windows**, enrutamiento, conmutación y el **direccionamiento IP**.

Duración: 16 hrs.

Firewalls/VPNs y Seguridad Perimetral

01 Firewalls y clasificación

- Firewalls y el modelo **OSI/DOD**
- Análisis de la seguridad de **TCP/IP**

02 Aspectos importantes de TCP/IP: Datagramas y segmentos

- Datagramas: **ICMP**, **UDP**, **TCP**
- Herramientas **TCP/IP**: **ifconfig**, **ping**, **route**, **tracert**, **host**, **tcpdump**, **tcpshow**, **arp**, **netstat**, **nslookup**, **lsof**, **ip addr**
- Diseño e Implementación de **Firewalls**

03 Introducción a las VPNs

- Qué son las **VPNs**
- Requerimientos básicos
- Conceptos de tunneling

04 Tecnologías de encriptación

- Encriptación simétrica vs. asimétrica
- Funciones **hash**
- Algoritmos de encriptación y fortalezas relativas
- **DES, 3DES, AES, 3AES, Diffie-Hellman, El-Gamal, DSS**
- Firmas digitales y Certificados digitales
- Autoridades independientes vs. autoridades comerciales
- Criterios de diseño de redes **VPNs**

05 Arquitectura de Firewalls y VPNs

- Reenvío de paquetes y filtrado de paquetes
- **Firewalls**, Intranets y Zonas Desmilitarizadas (**DMZ**)
- Soluciones **Firewall**

06 Topologías OpenVPN

- Topología **Host a Host OpenVPN**
- Topología **RoadWarrior OpenVPN**
- Instalación y Configuración de **VPNs**

07 Funcionamiento de Firewall IPTables

- La tabla **Filter** y sus operaciones (**FORWARD**, **INPUT**, **OUTPUT**)
- Configuración de reglas **IPTables**
- Configuración de cadenas **INPUT**, **OUTPUT**, **IN**, **OUT**
- Arranque y baja de **IPTables**
- Objetivos **IPTables**: **ACCEPT**, **DROP**, **REJECT**, **LOG**
- Seguridad perimetral y Zona Desmilitarizada (**DMZ**)

08 Introducción a la seguridad perimetral y DMZ

- Diseñando un perímetro seguro y **DMZ**
- Reforzando la seguridad del perímetro y **DMZ**
- Monitoreo de la seguridad del perímetro y **DMZ**

09 Implementación de seguridad perimetral y DMZ con IPTables

- Reenvío de paquetes Traducción de direcciones (**NAT**)
- La tabla **NAT** (**Network address Translation**) y sus funciones **PREROUTING**, **POSTROUTING**
- Manejo de traducción de direcciones (**DNAT**, **SNAT**)
- Redireccionamiento de puertos y enmascaramiento
- Optimización del **Firewall** y manejo de errores
- Evaluando la seguridad perimetral y **DMZ**
- Prueba de **Firewalls** y Resolución de problemas

10 Protección avanzada de IPTables

- Buscar y detener tráfico sospechoso
- Definir reglas de acceso basadas en tiempo
- Protección de ataques **DOS, DDoS**
- Limitar el tamaño del registro
- Bloque de tráfico entrante de host o dominio

11 Herramientas de comprobación del Firewall



www.informaticaintegrada.mx