DIPLOMADO MASTER EN SEGURIDAD Y HACKING ÉTICO

Este diplomado es perfecto para aquellos profesionales que quieran incursionar en la **Seguridad de Tecnologías de Redes e Internet**, donde se examinarán técnicas de blindaje, encriptación, autentificación, control de acceso, análisis de tráfico, **Firewall/VPNs**, **Seguridad Wireless**, **Google Hacking Pentests** 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.

DIRIGIDO A:

Gerentes y directores del área de seguridad de la información, especialistas en TI, proveedores de Internet, administradores, gerentes de seguridad física y corporativa, profesionales de las áreas de computación, sistemas y comunicaciones que deseen actualizar sus conocimientos e implementar seguridad en sus centros de datos e **Internet/Intranet**.

BENEFICIOS:

- El egresado será capaz de implementar los nuevos esquemas de seguridad y buenas prácticas bajo la norma **ISO/IEC 27001**. Detectará vulnerabilidades e intrusos.
- Conocerá métodos para defenderse contra ataques **DDoS**, a contraseñas, puertas traseras (**Backdoors**), enmascaramiento IP, escaneo de puertos, **Web** y **DNS** mediante **Dnsspoof**.
- Implementará **VPNs**, **Firewalls** y **DMZ**.
- Estará apto para desarrollar estrategias que enfaticen la seguridad y resguardo de la información de su empresa.
- Hará frente a un sistema con software vulnerable desconocido y realizar ingeniería inversa para localizar el código problemático.

- Realizará penetración (**Pentest**), seguridad ofensiva y toma de control de sistemas.

INCLUYE:

- Instalaciones adecuadas
- Material y manuales de cursos
- Instructores Certificados
- Box lunch
- Servicio de cafetería continua
- Estacionamiento
- Registro **STPS**

MÓDULO 1 BLINDAJE AL SERVIDOR Y HACKING ÉTICO

Objetivo: Proveer al participante bases sólidas en la administración de la seguridad del sistema operativo y **Hacking Ético** usando herramientas de búsqueda de vulnerabilidades, sistemas de detección de intrusos, análisis de tráfico, además de revisar las últimas técnicas de ataques detección de intrusos (**IDS**), puertas traseras (**Backdoors**), ataques a **passwords** y las medidas de protección necesarios para evitarlos además de la implementación de buenas prácticas basadas en **ISO/IEC 27001**.

Dirigido a: Directores y auditores del área de seguridad TI, **Pentester, hackers Éticos**, profesionales de las áreas de computación, informática, sistemas y comunicaciones que deseen blindar su centro de datos.

Requisitos: Conocimientos básicos de Linux

Duración: 18 hrs.

Inversión: **$** 5,600

TEMARIO:

Introducción al Hacking Ético

- Elementos de seguridad
- Diferencia entre pruebas de penetración y **ethical hacking**
- Importancia del **hacker ético**
- Consideraciones

Problemática de Seguridad

- Problemas de Seguridad en Internet
- Vulnerabilidades, Amenazas y Ataques
- Amenazas y Ataques Famosos
- Arquitectura de Seguridad **OSI/DOD**
- Confidencialidad y Autenticación
- Integridad y Control de Acceso

Blindaje del sistema operativo

- Estándares de seguridad básicos para S.O de red
- Instalación, particiones y seguridad
- Particiones primarias, extendidas y lógicas
- Seguridad en la consola del servidor
- Manejo de cuentas de Administrador y súper-usuario
- Seguridad en cuentas y grupos de trabajo
- Administración del control de acceso
- Manejo de permisos y atributos de archivos y directorios
- Rutas de confianza y programas troyanos

Ataque a contraseñas

- Tipos de ataque
- Ataque a contraseñas basadas en diccionario y fuerza bruta
- **Crakeando** algoritmos de cifrado: **DES**, **MD5** y **Blowfish**

- **John the Ripper**: herramienta de ataques a contraseñas

Medidas proactivas y verificación de integridad de datos

- Detección de troyanos y código dañino
- Instalación y configuración de herramientas de integridad de archivos (**Tripwire**)
- Uso de sumas de comprobación (**Checksums**)
- Ataques relacionados con el registro

Monitoreo del tráfico de red y controles de Seguridad

- Señales y puertos privilegiados
- Gestión de la memoria virtual
- Barrido de puertos y el ping de la muerte
- Detectores de rastreo (**ICMP**, **UDP**)
- Cómo defenderse de ataques de **Sniffers** y **Scanners**

Sistema de detección de intrusos (IDS)

- Arquitectura de un **IDS**
- Sistema de detección de intrusos en Host (**HIDS**) y Red (**NIDS**)
- Dónde colocar el **IDS**
- **Snort** como **IDS**
- **Snort** en modo **Sniffer**, registro de paquetes y **NDIS**
- **Ataques de denegación de servicios (DoS)**
- Ataque **SYN** (inundación **TCP/SYN**)
- El ping de la muerte y ping **flood**

Ataque y defensa a servidores Web

- Por qué hackean los sitios Web?
- Vulnerabilidades del servidor Web y manipulación de URL
- Aprovechamiento de las debilidades de los identificadores de sesión
- Aprovechamiento de las debilidades de sistemas de autenticación
- Ataque Por Inyección (**Structured Query Language Injection**)

- Ataque de Denegación de Servicio (**DoS**)
- Ataque de fuerza bruta
- Inyección de scripts maliciosos **Cross-site Scripting (XSS)**

Ataque a bases de datos SQL

- **OWASP** (**Open Web Application Security Project**)
- Seguro eres vulnerable
- Cómo funciona **SQL Injection,**
- Tipos de inyección y usuarios malintencionados
- Atacando base de datos realizar consultas
- Realización de accesos ilegítimos
- Ejecución de comandos en el servidor, subida y lectura de archivos
- Rompiendo la integridad de datos almacenados
- Cómo evitar las vulnerabilidades por inyección **SQL**
- Revisando el código para vulnerabilidades de inyección por **SQL**
- Probando las Vulnerabilidades de **Inyección SQL Contents**

Ingeniería social

- Ingeniería Social y la seguridad informática?
- Técnicas de Ingeniería Social
- Robo de identidad
- Tácticas de intrusión y estrategias para prevención
- Riesgo de red social para redes corporativas

MÓDULO 2 — CONFIGURACIÓN DE REDES PRIVADAS VIRTUALES (VPNS)

Objetivo: Proveer al participante los conocimientos y herramientas necesarios para diseñar e implementar Redes Privadas Virtuales (**VPNs**) utilizando protocolos de seguridad bajo ambiente Linux.

Dirigido a: Directores y gerentes del área de Telecomunicaciones, Informática, auditores en Seguridad TI, **Pentesters, hackers Éticos,** profesionales de las áreas de computación, sistemas y comunicaciones que deseen implementar seguridad en redes corporativas a través de **VPNs**.

Requisitos: Conocimientos de Linux y redes TCP/IP.

Duración: 16 hrs.

Inversión: $ 4,800

TEMARIO:

Introducción a las VPNs

- Qué son las **VPNs**
- Requerimientos básicos
- Conceptos de **tunneling**
- Repaso a los protocolos **PPP**, **PPTP** y **L2TP**

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**

Topología Host a Host OpenVPN

- Generación de clave de encriptación
- Configuración del servidor y cliente

Topología Road Warrior OpenVPN

- Consideraciones preliminares
- Creando el CA
- Generación del certificado para el servidor
- Generación de la clave de encriptación para el servidor
- Generando certificados y claves privadas para los clientes
- El parámetro de **Diffie-Hellman**
- Configuración del servidor y cliente

Topología Red a Red OpenVPN

- Configuración de Servidor Red a Red
- Configuración de Cliente Red a Red

Consideraciones

- Usando **iptables-firewall** con **OpenVPN**
- **OpenVPN** y **Windows®**
- **OpenVPN** detrás de un proxy

Revisión de casos e implementación en laboratorio

MÓDULO 3 — CONFIGURACIÓN DE FIREWALLS Y SEGURIDAD PERIMETRAL

Objetivo: Proveer al participante los conocimientos para el manejo de tecnologías de filtrado de paquetes asociados a servicios de Internet, detección de puntos vulnerables, además del diseño, implementación y administración de Firewalls que permitan proteger las redes corporativas frente a posibles ataques.

Dirigido a: Gerentes y directores de seguridad, **Pentester, hackers Éticos,** profesionales de las áreas de computación, sistemas y comunicaciones que deseen implementar **Firewalls** para la protección de servidores corporativos.

Requisitos: Conocimientos de Linux y redes TCP/IP.

Duración: 18 hrs.

Inversión: $ 5,200

TEMARIO:

Introducción

- Funciones del **Firewall**
- Clasificación de **Firewalls**
- Firewalls y el modelo **OSI/DOD**
- Análisis de la seguridad de **TCP/IP**
- **Aspectos importantes de TCP/IP: Datagramas y segmentos**
- Datagramas: **ICMP**, **UDP**, **TCP**
- Herramientas **TCP/IP**: **ifconfig, ping, route, traceroute**, **host, nslookup**, **tcpdump**, **tcpshow**
- Diseño e Implementación de **Firewalls**

Arquitectura de Firewalls

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

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**)

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**

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

Protección avanzada de IPTables

- Buscar y detener tráfico sospechoso
- Definir reglas de acceso basadas en tiempo
- Protegemos de un tipo de "**buffer overflow exploits”**
- Limitar el tamaño del registro
- Bloque de trafico entrante de host o dominio

Herramientas de comprobación del Firewall

MÓDULO 4 PENTEST Y HACKING AVANZADO

Objetivo: Para finalizar tu entrenamiento, profundizamos el estudio de **Metasploit Unleashed**, **seguridad Inalámbrica**, **fuerza bruta**, **análisis de tráfico**, **Google® Hacking**, **anonimato de conexiones, Pentest** y **seguridad ofensiva** terminando con la toma de control de sistemas a través de la **explotación de vulnerabilidades**. Este curso te presenta las últimas herramientas de **hacking** y técnicas en el campo e incluye laboratorios donde se realizan pruebas de principio a fin.

Dirigido a: Aquellos profesionales de seguridad que desean realizar **Tests de Intrusión**, **Hacking Ético** y **Auditorías de Seguridad**.

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

Duración: 24 hrs.

Inversión: $ 7,500

TEMARIO:

Ethical Hacking

- Evaluación de seguridad
- **Ethical Hacking**
- Pruebas de penetración

Tipos de pruebas de penetración

- Clasificación de acuerdo al conocimiento previo de las pruebas
- Clasificación de acuerdo al lugar lógico de ejecución
- Clasificación de acuerdo al alcance

Responsabilidad ética y legal

- Comportamiento ético de un **pentester**
- Cliente
- **Pentester**
- Pensamiento de un **pentester**

Metodologías para realizar pruebas de penetración

- **PTES** ***(Penetration Testing Execution Standard)***
- **OSSTMM** ***(Open Source Security Testing Methodology)***
- **NIST 800-115** ***(National Institute Standards and Technology)***
- **ISSAF** ***(Information Systems Security Assessment Framework)***
- **PTF** ***(Penetration Test Framework)***

Planeación

- Entrevista con el solicitante
- Identificar activos críticos del negocio
- Determinar los objetivos de evaluación
- Autorización de la organización
- Acuerdo de confidencialidad
- Contrato

Fases de las pruebas de penetración

- Reconocimiento
- **Whois** y Registros Regionales de Internet
- Servidores y Zonas **DNS**

Recolección de datos

- Recolección de datos como:
- Rango de Red y **sub-red** (**Network Range** y **subnet mask**)
- Acertar maquinas activas
- Puertos abiertos y las aplicaciones que están corriendo en ellos
- Detectar versiones de Sistemas Operativos
- Nombres de Dominios (**Domain Names**)
- Bloques de Red (**Network Blocks**)
- Direcciones IP específicas
- País y Ciudad donde se encuentran los Servidores
- Información de Contacto (números telefónicos, emails, etc.)
- **DNS records**
- Tipos de **DNS Records**: **A** (**address**), **MX** (**mail exchange**)
- **NS** (**name server**), **CNAME** (**canonical name**),
- **SOA** (**start of authority**), **TXT** (text), **HINFO** (**host info**)

Herramientas de recolección de datos

- Escaneo de Vulnerabilidades
- Redes sociales y buscadores de personas
- **Google Hacking®**
- **Nslookup**, **dig**, **host**
- Herramientas en línea (Online)
- **Nmap**, **Nessus**, etc
- Análisis de vulnerabilidades
- Tipos de exploits
- Marcos de explotación

Metasploit Framework

- **Metasploit** a profundidad
- Arquitectura de **Metasploit**
- Manejo de **Mestasploit framework**
- **Kali Linux** y **Metasploit framework**
- Detección de redes y ejecución de exploits
- **Information gathering**
- Interactuando con **MSF** (**msfconsole, msfcli, msfgui, msfweb**)
- Obteniendo Información y Análisis de Vulnerabilidades
- Escribiendo un simple **Fuzzer** y **X11** a la escucha
- Manejo de herramientas **NeXpose** y **Nessus**
- La evidencia recogida
- **IDS/IPS** la evasión

Spoofing (suplantación de identidad)

- Falsear información
- Engañar
- Obtener información de un usuario determinado
- Comprometer un sistema de red
- Crear confusión haciendo aparentar cosas que no son reales
- Tipos de **Spoofing: ARP Spoofing**, **IP Spoofing**, **Mail Spoofing**, **DNS Spoofing**, **Web Spoofing**

Ataque Man in the middle (MITM)

- Ataque de hombre en medio
- Herramientas para hacer un **MITM**
- **PacketCreator, Ettercap**, **Dsniff, Kali Linux**
- protegerse de un ataque **MITM**

Pruebas de penetración a redes inalámbricas

- Arquitectura de redes **Wi-Fi**
- Modo infraestructura (**BSS**) y Modo **Ad-Hoc** (**IBSS**)
- Hardware inalámbrico(**antenas**, **tarjetas, Access point**)
- La familia de protocolos **IEEE 802.11**
- Vulnerabilidades en redes inalámbricas
- Denegación de servicio
- Tipos de ataques de denegación de servicio
- **Access Points** no autorizados
- Intercepción/Captura de tráfico y ataques criptográficos
- Ataque **Evil Twin**
- Protocolos de cifrado
- Cifrados **WEP** y **WPA/WPA2**

Después de la explotación

- **Command Shell** y acceso a la terminal
- **Backdoor Shell** y **Backdoor Shell inverso**
- Comparativa de marcos de explotación

Documentación

- Resumen ejecutivo
- Objetivos
- Alcance
- Hallazgos
- Recomendaciones
- Anexos