



Diplomado en Ethical Hacking

Diplomado en **Ethical Hacking**

Introducción

Con la certificación Ethical Hacking conocerás las técnicas del Hacking Ético, sus características, funcionalidades y alcances con la finalidad de defender a las organizaciones contra los ciberataques. Utilizarás las herramientas, metodologías y técnicas más utilizadas en Ingeniería Social, con la finalidad de detectar este tipo de ataques en entornos reales a través de casos prácticos. Conocerás como realizar búsqueda de información en las diferentes fuentes públicas, así como el uso de herramientas de seguridad para encontrar información confidencial. Realizaras análisis de las redes para identificar el mapeo de red, sistemas operativos, versiones y puertos abiertos, identificando los activos. Conocerás como analizar las vulnerabilidades más comunes de los sistemas operativos explotando en un ambiente controlado. Conocerás las técnicas del Hacking Ético, sus características, funcionalidades y alcances con la finalidad de defender a las organizaciones contra los ciberataques. Y aprenderás como redactar un informe ejecutivo y técnico para la presentación de los hallazgos encontrados, donde genere valor con recomendaciones de mitigación.

Objetivos de aprendizaje

El objetivo del curso es aprender a realizar Pentesting de manera profesional siguiendo metodologías con un enfoque ético, conociendo las técnicas de ataque que realiza un ciberdelincuente para prevenir brechas de seguridad, aprenderás a identificar vulnerabilidades en los activos tecnológicos, dando recomendaciones para su mitigación.

Puntos específicos

- Comprender las tendencias de seguridad actuales.
- Conocer los elementos de seguridad de la información.
- Comprender los conceptos, tipos y fases de ethical hacking.
- Gestionar las amenazas a la seguridad de la información.
- Desarrollar estrategias para la comprensión, gestión y protocolos de los vectores de ataque.
- Dominar los conceptos, tipos y fases de pentesting.
- Comprender el proceso de pentesting.
- Dominar los controles de seguridad de la información.

Al finalizar el curso, el estudiante tendrá los conocimientos necesarios para poder realizar pruebas de intrusión de forma profesional en la infraestructura tecnológica, siguiendo metodologías con enfoque 100% ético siendo un profesional de alto valor con uno de los perfiles más demandado por las empresas.

Público Objetivo

Estudiantes, auditores, analistas de seguridad, consultores o asesores en temas de auditoría y de control interno y gestión de riesgos y profesionales vinculados al mundo de la ciberseguridad.

Requisitos Previos

- No hay requisitos previos formales para esta certificación.

Formación

- Tipo de curso: Profesional
- Código de certificación: CEHPC™
- Vencimiento: 3 años

Contenido

Módulo 1:

1. Fundamentos de Pentesting y Hacking Ético

1.1 Introducción al Hacking Ético

Que es un Hacker

Tipos de Hackers

Clasificación de Hackers

Hacking vs Hacking Ético

El Proceder de un Hacker

¿Cómo lo hacen?



RISKGROUP
INSTITUTE



1.2 Penetration Testing

Que es el Penetration Testing
Importancia del Pentesting
Conocimiento del Pentester
Tipos de Prueba de Pentesting
Categorización de un Pentesting
Metodologías de Pentesting
Fases Pentesting

1.3 Metodologías y Buenas Practicas

PETS
OWASP
MITRE ATT&CK

1.4 Tecnologías y herramientas para la Seguridad

IPS / IDS
VPN
Sistemas de filtrado de Contenido
Routers
Switches
Firewall
HoneyPot
Respuesta a incidentes de Seguridad de la Información
SIEM
Respaldo y Recuperación

Módulo 2:

2. Ingeniería Social

2.1 Historia de la Ingeniería social

¿Qué es la Ingeniería Social?
¿Cómo funciona la Ingeniería Social?
Canales que utilizan los atacantes
Métodos que utilizan los atacantes
Factores que hacen que las empresas sean vulnerables a los ataques

2.2 Tipos de ingeniería social

Phishing
Planificación de phishing
¿Como se ve?
Spear Phishing
Vishing

Smishing
Whaling
Baiting
Scareware
Pretexting

2.3 Protección y medidas de control

Política de Uso Aceptable
Medidas de revisión preliminar
Concienciación y Formación
Campañas de phishing

Módulo 3:

3. Reconocimiento Pasivo e Activo

3.1 Reconocimiento Pasivo

Framework OSINT
Google Hacking
Recolección de DNS
Whois
Shodan

3.2 Reconocimiento Activo

Escaneo y enumeración de red
Puertos y Servicios
Clasificación del tipo de respuesta al escanear puertos

Módulo 4:

4. Escaneo y Análisis de Red

4.1 Introducción al análisis de red

Ping
Traceroute
Barrido de Ping
Tipo de Puertos
El Protocolo de control de mensajes de Internet (ICMP)
SYN /ACK
Indicadores de comunicación TCP
Banderas de comunicación TCP
Método Three-wayhandshake

4.2 Instalación Ambiente de trabajo

Instalación de Wmware
Instalación de Kali Linux.
Actualización del Sistema
Creación de Usuario
Instalación metasploitable 2 y 3

4.3 Introducción a NMAP

¿Qué es NMAP?
Escaneo de Nmap Básico
Opciones de NMAP

4.4 Categorías a NMAP

Host Discovery– Descubrimiento de host
Scan Techniques– Técnicas de escaneo
Port Specification And Scan Order – Especificaciones de puertos y orden de escaneo
Service/Version Detection- Detección de Servicios/Versiones
OS Detection– Detección de Sistema Operativo
Timing and Performance– Tiempo y Rendimiento
Firewall/IDS Evasion And Spoofing
Output

Módulo 5:

5. Análisis de Vulnerabilidades

5.1 Introducción a las Vulnerabilidades

Que es Análisis de Vulnerabilidades
¿Qué son las vulnerabilidades?
¿Que es CVSS?

5.2 Escaneo de vulnerabilidades automatizado

Nessus
ZAP

5.3 Escaneo de vulnerabilidades manual

Escaneo con NMAP Scripts

Módulo 6:

Explotación

6.1 Metasploit

Que es metasploit
Comandos Básicos
Búsqueda de sploit
Ejecución de meterpreter

Módulo 7:

Técnicas de Ataque

7.1 Tipos de Ataque

Malware
Spoofing
Man-in-the-middle
Denegación de servicio distribuido (Ddos)
PiggyBacking
Inyección de Código SQL
Phishing

Módulo 8:

Informe de Resultados

Aprenderás como redactar un informe ejecutivo y técnico para la presentación de los hallazgos encontrados, donde genere valor con recomendaciones de mitigación.

8.1 Contenido de un informe

Informe Técnico
Informe Ejecutivo