Temario CertiProf.

Certificación Internacional

Ethical Hacking Professional Certification - CEHPC™

Esta certificación está diseñada para dotar a los profesionales de las habilidades y los conocimientos necesarios para analizar y mitigar vulnerabilidades en los sistemas de seguridad de la información.



Información del programa.

Objetivos del programa.

- Comprenderás las fases del hacking ético y del proceso de pruebas de penetración.
- Identificarás y gestionarás amenazas y vectores de ataque en entornos informáticos.
- Desarrollarás estrategias para comprender y gestionar protocolos de vectores de ataque.
- Comprenderás los conceptos, tipos, fases y proceso de pentesting.
- Aplicarás controles de seguridad de la información para proteger sistemas y redes contra ataques maliciosos.

Perfil del participante.

- Estudiantes, auditores y analistas de seguridad que desean comprender las técnicas y fundamentos del hacking ético.
- Consultores y asesores en auditoría, control interno y gestión de riesgos tecnológicos.
- Profesionales de ciberseguridad que necesitan adquirir o fortalecer sus habilidades en pentesting y mitigación de amenazas.

Para mayor información contactar:

+503 7840-2073 info@inmersiongroup.com

Immersion
International Business School

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?

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.

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.

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.

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 Categorias a NMAP.

- Host Discovery– Descubrimiento de host.
- Scan Techniques– Técnicas de escaneo.

- Port SpecificationAnd Scan Order – Especificaciones de puertos y orden de escaneo.
- Service/Version Detection- Detecciónde Servicios/Versiones.
- OS Detection– Detección de Sistema Operativo.
- Timing and Performance– Tiempo y Rendimiento.
- Firewall/IDS Evasion And Spoofing.
- Output.

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.

6. Explotación.

6.1 Metasploit.

- Que es metasploit.
- Comandos Básicos
- Búsqueda de sploit.
- Ejecución de meterpreter.

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.

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.

Conoce más sobre nosotros.

Somos tu aliado para transformar el aprendizaje en éxito profesional.

Somos **Immersion International Business School.** Ofrecemos soluciones integrales y trabajamos para potenciar el talento humano y fortalecer a las empresas, ayudándolas a transformar desafíos en oportunidades.

Elige tu modalidad

Programas abiertos.

Accesibles a diferentes empresas con objetivos de aprendizaje en común.

Programas cerrados.

Se adaptan y enfocan a los objetivos y necesidades de cada empresa.

Tenemos presencia en



Nuestros servicios

Capacitaciones

Diseñadas para impulsarte.

Certificaciones

Avaladas internacionalmente.

Consultorías

Personalizadas para tu caso.

Somos #CertiProfPartner

En la actualidad, somos Training v Autorizado de CertiProf, un líder dedicado formar profesionales, potenciando sus habilidades en el ámbito laboral.

Hemos sido aprobados para brindar un servicio de calidad y ayudarte a alcanzar tus objetivos profesionales.

certiprof®
Certified Partner For Learning Solutions

Para mayor información contactar:

+503 7840-2073 info@inmersiongroup.com

Immersion
International Business School