CIBERTEC

CURSO
ETHICAL HACKING

64 HORAS ACADÉMICAS

ONLINE

Protege sistemas aprendiendo a hackearlos éticamente.

Conviértete en un experto en detección de vulnerabilidades con herramientas de hacking ético Open Source. Aprende a identificar, analizar y explotar fallas de seguridad en servidores y aplicaciones web. Domina metodologías prácticas usadas por profesionales del Ethical Hacking a nivel global.

¿A QUIÉN ESTÁ DIRIGIDO?

Profesionales, egresados y estudiantes interesados en iniciarse en un proceso de Ethical Hacking.

¿QUÉ LOGRO CON EL CURSO?

Al finalizar el curso, podrás desarrollar soluciones prácticas para optimizar tareas diarias y estar preparado para:

- Identificar vulnerabilidades en sistemas y redes desde entornos internos (LAN) y externos (Internet)
- Aplicar pruebas de penetración con metodologías como OSSTMM en entornos controlados.
- Reconocer estrategias de prevención y mitigación de riesgos en seguridad informática.

¿QUÉ CERTIFICADO OBTENGO?

Al aprobar la capacitación, el alumno obtendrá un certificado de Cibertec:

- Ethical Hacking

CIBERTEC

CONTENIDO TEMÁTICO

1 Introducción al Ethical Hacking

- Conceptos básicos de ciberseguridad
- Normativa sobre ciberseguridad (ISO, GDPR, CFAA, normativa peruana)
- Equipos de ciberseguridad y roles
- Tipos de hacking (ético, sombrero blanco, negro y gris).
- Metodologías de Evaluación

2 Linux para Ethical Hacking

- Consola de Linux y comandos básicos
- Sistema de archivos y permisos
- Instalación de herramientas esenciales

3 Seguridad en protocolos y redes

- Protocolos TCP/IP y vulnerabilidades comunes
- Análisis de tráfico con Wireshark
- Uso de netcat y scapy para pruebas de red
- Ataques de red (MITM, ARP spoofing)

4 Creación de un laboratorio para Ethical Hacking

- Planificación y configuración de entornos virtualizados
- Configuración de Kali Linux y Metasploitable
- Simulación de redes y entornos vulnerables

5 Reconocimiento y recolección de Información

- Uso de Google Hacking y motores de búsqueda.
- OSINT (Open Source Intelligence) y herramientas de reconocimiento
- Interrogación DNS y reconocimiento pasivo

6 Escaneo y enumeración de objetivos

- Escaneo de Puertos
- Enumeración de Servicios
- Nmap

7 Análisis de Vulnerabilidades

- Analizadores a nivel plataforma
- Analizadores a nivel aplicación
- Vulnerabilidades conocidas

8 Explotación de vulnerabilidades

- Exploits
- Metasploit
- Framework
- Password Cracking

9 Buenas prácticas y prevención de ataques

- Estrategias de mitigación de vulnerabilidades
- ¿Qué es el análisis forense básico?
- ¿Qué es el principio de defensa en profundidad?

¿POR QUÉ ELEGIR CIBERTEC?

Instituto N° 1 en tecnología con equipos de vanguardia.

Docentes especializados con estándares internacionales.

aws · cisco · ITIL

Respaldo de empresas top internacionales.

Más de 90 cursos, especializaciones y actualizaciones.

Tecnología como núcleo para el desarrollo de programas.