

Curso de Hacking Ético y Ciberseguridad

Objetivo: Enseñar los principios básicos del hacking ético, identificación de vulnerabilidades y ejecución de pruebas de penetración (Pentesting) para blindar sistemas.

Plan de Evaluación: Curso presencial práctico mediante la realización de ejercicios en clase y evaluadas por Ingeniería Digital CA.

Duración del Curso: 24 Horas Académicas de 45 minutos cada hora. 6 Clases

Perfil del Estudiante: Estudiantes o profesionales de Informática o afines

Contenido del Curso

MÓDULO 1: FUNDAMENTOS Y RECONOCIMIENTO (Clases 1 y 2)

- **Introducción al Hacking Ético:** Marco legal, ética y tipología de atacantes.
- **Entorno de Combate:** Fundamentos de virtualización, despliegue de laboratorio seguro y arquitectura de Kali Linux.
- **Dominio de la Terminal:** Supervivencia en la línea de comandos (Linux) y control de sistemas sin interfaz gráfica.
- **Práctica(Wargames):** Navegación en servidores remotos y ejercicios de escalada de privilegios básicos.

MÓDULO 2: VULNERACIÓN DE SISTEMAS (Clases 3 y 4)

Objetivo: Detectar la debilidad y romper la defensa.

- **Inteligencia de Objetivos:** Uso de escáneres (Nmap) para descubrir equipos activos, puertos y servicios ocultos en la red.
- **Análisis de Vulnerabilidades:** Identificación de fallos de seguridad explotables.

- **Arsenal de Explotación:** Uso de **Metasploit Framework** y ataques de fuerza bruta controlados.
- **Práctica (Live Fire):** Mapeo de red en vivo e infiltración técnica en el servidor objetivo "Metasploitable 2".

MÓDULO 3: OPERACIONES REALES (Clases 5 y 6)

Objetivo: Simulación de escenario real, post-explotación y reporte.

- **Post-Explotación:** ¿Qué hace un hacker una vez que está dentro? (Persistencia, control remoto y exfiltración de datos).
- **Hacking Web & Automatización:** Uso de OWASP ZAP / Burp Suite para detectar fallos en aplicaciones web.
- **El Reto Final (CTF):** Ejercicio "Capture The Flag". Ataque en tiempo real donde el alumno debe capturar un objetivo en un sistema seguro sin asistencia.