



# CURSO ETHICAL HACKING

Plan de estudio



educación 





## Nuestro propósito

**Transformar positivamente la vida de las personas.**

Queremos que seas protagonista en la transformación que estamos viviendo. Por eso, nos comprometemos a capacitarte para que estés al día con las necesidades digitales actuales.

Te invitamos a trabajar en conjunto para que descubras tu mejor versión y la potencies. Anímate, toma las riendas de tu futuro.

Code your future!

## Contenido del curso

Aprende las técnicas para analizar la seguridad de las redes empresariales. Maneja conceptos como vulnerabilidad y exploit para asistir a las organizaciones.

## Proyecto Integrador

### Pentesting en entornos controlados: aplicación práctica con IA

Aplicarás técnicas de ethical hacking con una máquina vulnerable (Metasploitable2) y herramientas de inteligencia artificial para optimizar tareas.

- Crearás una herramienta de ethical hacking asistida por IA.
- Enumerarás servicios y vulnerabilidades utilizando nmap y exploit DB.
- Documentarás hallazgos y generarás informes profesionales de pentesting.
- Explotarás vulnerabilidades reales, como en servicios IRC.
- Realizarás escaneos de seguridad automatizados con Nessus.
- Realizarás cracking de contraseñas, identificando hashes y aplicando técnicas de fuerza bruta con John The Ripper.

Este proyecto, con casos de uso reales, formará parte de tu portfolio personal, y te servirá como experiencia profesional. Al finalizar, podrás compartir el diploma en LinkedIn para destacar tu perfil utilizando @educacionit desde tus redes.

## ¿Qué aprenderás?

- Reconocimiento de vulnerabilidades.
- Ubicación y proveedor a través del IP.
- Identificación de servidores de y DNS.
- Escaneo y explotación.
- Exploits, payloads y shellcode.
- Utilización de Metasploit y Meterpreter.
- Instalación de keyloggers.
- Post-explotación.
- Credenciales y eliminación de logs.
- Client-side exploits.

# Plan de estudios

**1**

## Reconocimiento

- Whois.
- NS y MX.
- Transferencias de zona.
- Fuerza bruta de DNS.
- Virtual hosts.
- Geolocalización.
- Mapeo de IP a ASN.
- Shodan, Censys y Fofa.
- Google hacking.
- Direcciones de email de un dominio.
- Análisis de metadatos.
- Cabeceras de correos electrónicos.

**2**

## Escaneo y explotación

- Detección de puertos abiertos.
- Detección de SO y versiones de software.
- Scripts para detección de vulnerabilidades.
- Transferencia de archivos con Netcat.
- Conexión con shell de sistema.
- Shell bind y shell inversa.
- CVE, CWE y CVSS.
- Descarga y uso de exploits.
- Modificación de exploits.
- IA para reconocimiento avanzado.

- IA para escanear dominios y redes.
- Análisis automatizado de metadatos.

### 3

## Metasploit

- Metasploit y msfconsole.
- Selección y configuración de exploits.
- Selección y configuración de payloads.
- Explotación.
- Manejo de sesiones y upgrade a Meterpreter.
- Migración de procesos.
- Gestión de archivos desde Meterpreter.
- Generación de exploits con IA.
- Automatización inteligente de payloads.
- Optimización de escaneos con IA.

### 4

## Post-explotación

- Persistencia.
- Automatización.
- Elevación de privilegios.
- Enumeración de aplicaciones instaladas.
- Obtención de credenciales.
- Análisis predictivo de credenciales.
- Eliminación de logs.
- Port-forwarding.
- Explotación a través de otro equipo.
- Metasploit resource files.
- Meterpreter resource files.

**5**

## Client side exploits

- Payloads ejecutables.
- Conexión a una shell de Netcat.
- Ataque a Internet Explorer.
- Ataque a Adobe PDF Reader.
- Explotación de EternalBlue.
- Migración de Meterpreter a 64-bits.
- Obtención de credenciales desde la memoria.
- Vuelco de hashes de contraseñas.
- Crackeo de contraseñas con John The Ripper.
- Evasión de antivirus.

**6**

## Cracking local y remoto

- Identificación de tipo de hash.
- Análisis de hashes.
- Uso de wordlists en John The Ripper.
- Reglas de crackeo.
- Técnicas de fuerza bruta.

## Modalidad del Curso

### Duración

5 semanas / 18 h

### Frecuencia semanal

2 encuentros de 2 h

### Modalidad

Online en vivo

### Grupos reducidos

Promedio 15 personas

## Nivel: Intermedio





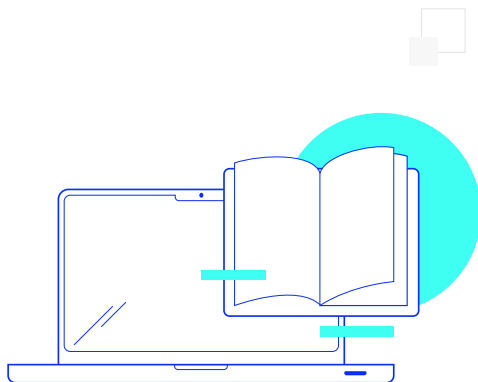
## Requisitos

Es recomendable tener una base sobre:

- **Introducción a la Ciberseguridad**
- **Criptografía y Blockchain**
- **Seguridad en Redes: Network Hacking**

## Dedicación fuera de clase

Además de las horas de clase, recomendamos que inviertas 4 h semanales extras para realizar los desafíos complementarios, estudiar el material de lectura y completar los exámenes del Alumni.



## ¿Cómo será tu experiencia?



### Aprender haciendo

Ejercita y pon en práctica lo estudiado.



### Trabajo en equipo

Une esfuerzos y potencia los resultados.



### Clases grabadas

Consúltalas las veces que quieras.



### Profesores expertos

Aprende de gigantes de la industria.



### Asistente académico

Recibe soporte dentro y fuera de clase.



### Plataforma Alumni

Encuentra recursos, materiales y clases.

## ¿Por qué Educación IT?



### IT Créditos

Gana puntos al aprobar los exámenes de los cursos. Luego, podrás canjearlos por nuevos cursos sin costo alguno. Los IT Créditos que acumules no vencen ni se devalúan.



### Garantía de aprendizaje

Si necesitas reforzar conceptos, recuperar clases o no estás satisfecho, ¡vuelve a tomar el curso sin ningún costo! Puede ser de forma total o parcial.



### Comunidad en Discord

Mantente en contacto con la comunidad de EducaciónIT a través de nuestro servidor de Discord. Podrás hablar con tus compañeros, profesores, asistentes académicos y soporte.



### Career Advisor

Ingresa al mundo laboral junto a nuestros asesores de carrera: crea un CV que impacte, arma y comparte tu portfolio en LinkedIn y Behance y ten simulacros de entrevistas.

## Preguntas frecuentes

**Si me pierdo una o más clases, ¿puedo recuperarlas?**

Todas las clases quedan grabadas de por vida en tu plataforma Alumni. ¡Siempre podrás volver a verlas cada vez que lo necesites!

**¿Cómo voy a aprender?**

Te enfrentarás a situaciones de trabajo reales, en donde tendrás que aplicar lo aprendido de forma individual y en equipo. Por medio de la prueba y el error, irás superando desafíos y obteniendo nuevas habilidades que luego podrás aplicar en el ámbito laboral.

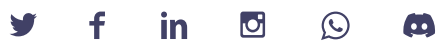
**¿Cómo son las clases online en vivo?**

Las clases duran entre 2 y 3 horas de lunes a viernes (sábados 3 o 4 hs) y se desarrollan de forma online en vivo en aulas virtuales, donde vas a poder interactuar con el instructor y tus compañeros.

Manejamos cupos reducidos para que puedas tener un seguimiento más personalizado durante tu aprendizaje.



[www.educacionit.com](http://www.educacionit.com)



@educacionit

---