



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 más utilizadas para analizar la seguridad de las redes empresariales. Maneja conceptos como Vulnerabilidad y Exploit para asistir a las organizaciones.

Prácticas en clase

Realizaremos prácticas para identificar los sistemas de una organización, así como para geolocalizar cada uno de los mismos. Haremos escaneos de puertos con Nmap, identificaremos los sistemas operativos y versiones de software, para luego buscar vulnerabilidades asociadas a dichas soluciones. Una vez hecho eso aprenderemos a explotarlas, principalmente utilizando Metasploit, trabajando sobre vulnerabilidades como ?EternalBlue? (MS17-10). También controlaremos los equipos víctima y aprenderemos a obtener información sensible, como credenciales y archivos confidenciales. También aprenderemos a infectar archivos benignos para transformarlos en maliciosos y que nos den acceso remoto a los equipos, así como también aprenderemos a utilizar los equipos ya controlados para atacar a otros equipos de la red.

¿Qué aprenderás?

- Fundamentos de la metodología Hacking
- Reconocimiento de vulnerabilidades
- Cómo identificar ubicación y proveedor a través del IP
- Identificación de servidores de eMail y DNS
- Trabajar con Escaneo y Explotación
- Buffer Overflow, Exploit y Shellcode
- Utilización de Metasploit
- Instalación de Keyloggers
- Post Explotación
- Saltar User Account Control
- Obtención de 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
- Google Hacking
- Obtener 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
- Ejecución de Scripts para detección de vulnerabilidades
- Transferencia de archivos con netcat
- Conexión con shell de sistema
- Shell Bind y Shell Inversa
- CVE, CWE y CVSS

- Descargar y usar exploits
- Modificación de exploits

3

Metasploit

- Msfconsole y configuración de la base de datos
- Búsqueda de exploits
- Selección y configuración de exploits
- Selección y configuración de payloads
- Explotación
- Payloads staged vs non-staged
- Manejo de sesiones y upgrade a Meterpreter
- Migración de procesos
- Gestión de archivos desde Meterpreter
- Obtener información del sistema
- Instalación de Keyloggers

4

Post Explotación

- Saltar User Account Control
- Persistencia
- Elevación de Privilegios
- Exploits Locales
- Enumerar aplicaciones Instaladas
- Obtener credenciales
- Eliminación de Logs
- Port Forwarding

- Explotación a través de otro equipo
- Metasploit resource files
- Meterpreter resource files

5

Client Side Exploits

- Payloads Ejecutables
- Conectarnos con metasploit a una shell de netcat
- Infección de ejecutables existentes con msfvenom
- Payloads en VBS
- Ataque a Internet Explorer
- Ataque a Adobe PDF Reader
- Payloads multiplataforma con Java
- Explotación de EternalBlue
- Migración de Meterpreter de 03- bits a 06- bits
- Obtener credenciales desde la memoria
- Volcar hashes de contraseñas
- Crackear contraseñas con John The Ripper

6

Cracking Local y Remoto

- Identificar tipo de hash
- Utilizar Wordlists en John The Ripper
- Reglas de Crackeo
- Generación de diccionarios personalizados
- Cracking de VNC
- Cracking de POP03-

- Cracking de FTP
- Cracking de SNMP

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



Principiante

Intermedio

Avanzado

Experto

Requisitos

Cursos o contenidos requeridos:

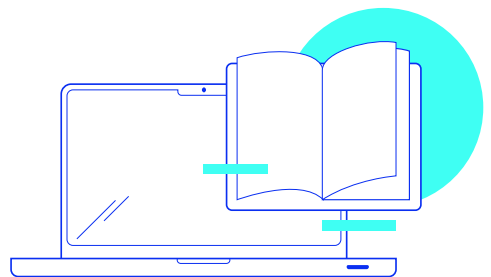
Introducción a la seguridad Informática

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

Ingresas 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



@educacionit