PROGRAMA DE ESTUDIOS

CEGOS

ETHICAL HACKING

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.

Modalidad del Curso

Duración

18 horas

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

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.

¿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.

¿Por qué en CEGOS?

Garantia de Aprendizaje
Puedes recursar sin cargo adicional si necesitas reforzar conceptos, recuperar clases o no estás satisfecho, puede ser de forma total o parcial.

Profesores Expertos
Profesionales certificados internacionalmente que trabajan con la tecnología y son referentes en su sector.

Plataforma Alumni
Espacio virtual donde encontrarás todo el material educativo, recursos, videos de clases grabadas, evaluaciones y más.

Orientación Profesional
Ingresa al mundo laboral, crea un CV que impacte, comparte tu portfolio en LinkedIn y realiza simulacros de entrevistas.

Bolsa de Trabajo
Postula a empresas líderes en su rubro que buscan talento en Latinoamérica y el mundo.

MODALIDAD ONLINE
EN VIVO

El aprendizaje a distancia en CEGOS está basado en la enseñanza presencial, un instructor dicta las clases utilizando un aula virtual en un horario establecido, las clases duran entre 2 a 3 horas de Lunes a Viernes y Sábados de 3 a 4 horas, las mismas se desarrollan en tiempo real donde podrás interactuar con el instructor y tus compañeros, se maneja cupos reducidos para que puedas tener un seguimiento más personalizado durante tu aprendizaje.

BENEFICIOS

- Material digital en plataforma Alumni.
- Acceso ilimitado a plataforma educativa.
- Videoconferencia en tiempo real.
- Grabación de clases ejecutadas.
- Docente certificado internacionalmente.
- Certificado de aprobación emitido por CEGOS.
- Factura impuestos de ley.
- Garantía de aprendizaje.

CERTIFICACIÓN

- Rúbrica de autoridades competentes
- Datos personales del alumno
- Carga horaria
- Plan de estudios
- Nota final

Autorizado por:

ATC AUTHORIZED Training Center

PMI Project Management Institute

Microsoft Partner Silver Learning

PROMETRIC

PEARSON VUE

CEGOS

Conocimiento para el desarrollo