TEC

Curso de preparación para:

Ethical Hacking Professional Certification (CEHPC)

II Semestre 2024
Programa Actualización Empresarial

HOY VIVO LA FORMACIÓN TEC

PRESTIGIO RESPALDO INNOVACIÓN

JUSTIFICACIÓN

Con la certificación Ethical Hacking conocerás las técnicas del Hacking Ético, sus características, funcionalidades y alcances con la finalidad de defender a las organizaciones contra los ciberataques. Utilizarás las herramientas, metodologías y técnicas más utilizadas en Ingeniería Social, con la finalidad de detectar este tipo de ataques en entornos reales a través de casos prácticos. Conocerás como realizar búsqueda de información en las diferentes fuentes públicas, así como el uso de herramientas de seguridad para encontrar información confidencial. Realizaras análisis de las redes para identificar el mapeo de red, sistemas operativos, versiones y puertos abiertos, identificando los activos. Conocerás como analizar las vulnerabilidades más comunes de los sistemas operativos explotando en un ambiente controlado. Conocerás las técnicas del Hacking Ético, sus características, funcionalidades y alcances con la finalidad de defender a las organizaciones contra los ciberataques. Conocerás las técnicas del Hacking Ético, sus características, funcionalidades y alcances con la finalidad de defender a las organizaciones contra los ciberataques. Y aprenderás como redactar un informe ejecutivo y técnico para la presentación de los hallazgos encontrados, donde genere valor con recomendaciones de mitigación.

OBJETIVO GENERAL

El objetivo del curso es aprender a realizar Pentesting de manera profesional siguiendo metodologías con un enfoque ético, conociendo las técnicas de ataque que realiza un ciberdelincuente para prevenir brechas de seguridad, aprenderás a identificar vulnerabilidades en los activos tecnológicos, dando recomendaciones para su mitigación.

Puntos específicos

- Comprender las tendencias de seguridad actuales.
- Conocer los elementos de seguridad de la información.
- Comprender los conceptos, tipos y fases de ethical hacking.
- Gestionar las amenazas a la seguridad de la información.
- Desarrollar estrategias para la comprensión, gestión y protocolos de los vectores de ataque.
- Dominar los conceptos, tipos y fases de pentesting.

- Comprender el proceso de pentesting.
- Dominar los controles de seguridad de la información.

Al finalizar el curso, el estudiante tendrá los conocimientos necesarios para poder realizar pruebas de intrusión de forma profesional en la infraestructura tecnológica, siguiendo metodologías con enfoque 100% ético siendo un profesional de alto valor con uno de los perfiles más demandado por las empresas.

PERFIL ACADÉMICO

Perfil de Entrada:

El curso está dirigido a profesionales de cualquier campo o área de gestión interesados en desarrollar los conocimientos necesarios para lograr la aprobación del examen de certificación internacional propuesto.

La persona que desee ingresar al curso no requiere conocimiento previo alguno.

Perfil de Salida:

Al finalizar el curso, el estudiante podrá realizar el examen de certificación internacional para la acreditación por parte de Certiprof en el momento que desee.

CONTENIDOS DEL CURSO

Detalle de los contenidos:

1. Fundamentos de Pentesting y Hacking Ético

1.1 Introducción al Hacking Ético

- Que es un Hacker
- Tipos de Hackers
- Clasificación de Hackers
- Hacking vs Hacking Ético
- El Proceder de un Hacker
- ¿Cómo lo hacen?

1.2 Penetration Testing

- Que es el Penetration Testing
- Importancia del Pentesting
- Conocimiento del Pentester
- Tipos de Prueba de Pentesting
- Categorización de un Pentesting
- Metodologías de Pentesting
- Fases Pentesting

1.3 Metodologías y Buenas Practicas

- PETS
- OWASP
- MITRE ATT&CK

1.4 Tecnologías y herramientas para la Seguridad

- IPS / IDS
- VPN
- Sistemas de filtrado de Contenido
- Routers
- Switches
- Firewall
- HoneyPot
- Respuesta a incidentes de Seguridad de la Información
- SIEM
- Respaldo y Recuperación

2. Ingeniería Social

2.1 Historia de la Ingeniería social

- ¿Qué es la Ingeniería Social?
- ¿Cómo funciona la Ingeniería Social?
- Canales que utilizan los atacantes
- Métodos que utilizan los atacantes
- Factores que hacen que las empresas sean vulnerables a los ataques

2.2 Tipos de ingeniería social

- Phishing
- Planificación de phishing
- ¿Como se ve?
- Spear Phishing
- Vishing
- Smishing

- Whaling
- Baiting
- Scareware
- Pretexting

2.3 Protección y medidas de control
- Política de Uso Aceptable
- Medidas de revisión preliminar
- Concienciación y Formación
- Campañas de phishing

3. Reconocimiento Pasivo e Activo

3.1 Reconocimiento Pasivo
- Framework OSINT
- Google Hacking
- Recolección de DNS
- Whois
- Shodan

3.2 Reconocimiento Activo
- Escaneo y enumeración de red
- Puertos y Servicios
- Clasificación del tipo de respuesta al escanear puertos

4. Escaneo y Análisis de Red

4.1 Introducción al análisis de red
- Ping
- Traceroute
- Barrido de Ping
- Tipo de Puertos
- El Protocolo de control de mensajes de Internet (ICMP)
- SYN /ACK
- Indicadores de comunicación TCP
- Banderas de comunicación TCP
- Método Three-wayhandshake

4.2 Instalación Ambiente de trabajo
- Instalación de Wmware
- Instalación de Kali Linux.

- Actualización del Sistema
- Creación de Usuario
- Instalación metasploitable 2 y 3

4.3 Introducción a NMAP

- ¿Qué es NMAP?
- Escaneo de Nmap Básico
- Opciones de NMAP

4.4 Categorias a NMAP

- Host Discovery– Descubrimiento de host
- Scan Techniques– Técnicas de escaneo
- Port SpecificationAnd Scan Order – Especificaciones de puertos y orden de escaneo
- Service/Version Detection- Detecciónde Servicios/Versiones
- OS Detection– Detección de Sistema Operativo
- Timing and Performance– Tiempo y Rendimiento
- Firewall/IDS Evasion And Spoofing
- Output

5. Análisis de Vulnerabilidades

5.1 Introducción a las Vulnerabilidades

- Que es Análisis de Vulnerabilidades
- ¿Qué son las vulnerabilidades?
- ¿Que es CVSS?

5.2 Escaneo de vulnerabilidades automatizado

- Nessus
- ZAP

5.3 Escaneo de vulnerabilidades manual

- Escaneo con NMAP Scripts

6. Explotación

6.1 Metasploit

- Que es metasploit
- Comandos Básicos
- Búsqueda de sploit
- Ejecución de meterpreter

7. Técnicas de Ataque

7.1 Tipos de Ataque

- Malware
- Spoofing
- Man-in-the-middle
- Denegación de servicio distribuido (Ddos)
- PiggyBacking
- Inyección de Código SQL
- Phishing

8. Informe de Resultados

- Aprenderás como redactar un informe ejecutivo y técnico para la presentación de los hallazgos encontrados, donde genere valor con recomendaciones de mitigación.

8.1 Contenido de un informe

- Informe Técnico
- Informe Ejecutivo

Cantidad de horas: 16 horas

METODOLOGÍA

Dentro de esta modalidad, el proceso de enseñanza y aprendizaje seguirá una dinámica tele presencial, en la que se desarrollarán sesiones sincrónicas (on line) semanales en un horario establecido a través de la plataforma Microsoft Teams. Implicará el uso de recursos tecnológicos para el desarrollo de la actividad formativa.
En estas sesiones se realizarán actividades como explicaciones o exposiciones participativas, atención de consultas, seguimiento de avances, coordinación de trabajos colaborativos, entre otros.

La aplicación de la metodología involucrará:

- Sesiones sincrónicas Las clases sincrónicas tendrán una duración de ***cuatro horas por sesión***.

PERFIL DEL PROFESOR

Dr. Gabriel Silva Atencio.

Gabriel, posee una carrera como ingeniero de sistemas, tres maestrías en las áreas de proyectos, innovación y administración de empresas y dos doctorados (uno académico y otro honorifico) en dirección empresarial, adicionalmente cuenta con un gran número de certificaciones internacionales y artículos científicos en las áreas de estrategia digital y tecnologías emergentes. En la actualidad, se desempeña como uno de los líderes incumbentes y de mayor impacto en la región en la era digital, junto con el apoyo que brinda a nuestra universidad como parte del cuerpo académico en los programas de más alto nivel de nuestra institución.

CRONOGRAMA

- 18, 19, 25 y 26 de octubre

HORARIOS

- Viernes de 5:30 p.m. a 9:30 p.m.
- Sábado de 8:00 a.m. a 12:00 m.d.

COSTOS

¢ 175.000 + 2% I.V.A.

El precio **no incluye** el valor de la certificación, queda a cargo del estudiante tramitar directamente la prueba. Durante el curso, el facilitador le instruirá sobre el proceso para inscribirse en la prueba con Certiprof.

CONTACTOS

TEC

¡Viva la formación TEC!

PRESTIGIO
RESPALDO
INNOVACIÓN