CIBERTEC

CURSO
ETHICAL HACKING

DURACIÓN: **64 HORAS ACADÉMICAS**
MODALIDAD: **ONLINE**

En este curso podrás identificar y solucionar vulnerabilidades de seguridad en sistemas y redes, y brindar recomendaciones para mejorar la seguridad general de una organización y prevenir los ataques cibernéticos

I. DIRIGIDO A

- Profesionales y egresados, interesados en evaluar la seguridad de sistemas informáticos y redes utilizando técnicas y herramientas especializadas.

II. METODOLOGÍA

- El enfoque práctico-reflexivo de cada una de las sesiones virtuales en tiempo real, así como la participación de los estudiantes en un ambiente interactivo de clases moderado por el instructor, permitirá el aprendizaje de contenidos y su aplicación en la resolución de contextos reales, utilizando herramientas digitales para el aprendizaje significativo.

III. BENEFICIOS

- **Acceso a la plataforma de Microsoft Azure Lab Services, desde cualquier PC o laptop con una conexión de Internet de 2 Mbps como mínimo.**
- **La máquina virtual estará configurada con el software y hardware necesario, con velocidad 2.1 Gbps de navegación disponible para las sesiones de clases.**
- **Correo institucional de Cibertec.**
- **Office 365 Web (Word, Excel, Power Point, etc.)**
- **Acceso a Microsoft OneDrive y Microsoft Teams.**

IV. LOGROS DEL CURSO

Al finalizar el curso, el alumno será capaz de elaborar un informe de recomendaciones para mitigar los riesgos o vulnerabilidades de seguridad. Adicionalmente, estará preparado para:

- **Aplicar una metodología de detección de vulnerabilidades.**
- **Analizar las vulnerabilidades con herramientas especializadas.**
- **Ejecutar las pruebas de penetración y evaluación de la seguridad.**

V. CERTIFICACIONES

- Al aprobar la actualización obtendrás un certificado en **Ethical Hacking** a nombre de Cibertec.

CERTIFICACIONES ASOCIADAS

- Especialización en Seguridad de Redes

VI. PRERREQUISITOS

- Conocimiento de Windows (nivel básico)
- Conocimiento de conectividad de redes (nivel básico)
- Conocimiento de comandos Linux (nivel básico)
- Conocimiento de inglés técnico (nivel intermedio)

VII. CONCEPTOS Y TERMINOLOGÍA

- **OSSTMM**
- **OWASP**
- **CVSS**
- **Linux**
- **TCP/IP**
- **ARP**
- **Denegación de servicio**
- **Malware**
- **Interrogación DNS**
- **WHOIS**
- **Escaneo de puertos**
- **Enumeración de servicio**
- **NMAP**
- **SCRIPT**
- **ENGINE**
- **EXPLOIT**
- **NMAP NSE**
- **WHOIS**
- **Análisis vulnerabilidades**
- **Aplicaciones vulnerables**
- **OWASP TOP 10**
- **Password cracking**
- **Metasploit framework**
- **Vulnerabilidades Web**

CIBERTEC

CONTENIDO TEMÁTICO

1 Ethical Hacking

- Conceptos básicos
- Tipos y etapas
- Metodologías de evaluación: OSSTMM, OWASP, CVSS
- Consola de Linux
- Sistema de archivos
- Instalación de software

2 Seguridad en Protocolos

- Protocolos de TCP/IP
- Sning
- Address Resolution Protocol (ARP)
- Denegación de servicio
- Malware (Generación de Payloads para evasión antivirus)

3 Reconocimiento del objetivo

- Análisis de información en motores de búsqueda
- Interrogación DNS
- WHOIS
- Herramientas automatizadas

4 Scanning y enumeración

- Escaneo de puertos y enumeración de servicios.
- Usando herramientas de escaneo de puertos (NMAP).
- Aplicando scripts (NMAP,SCRIPT, ENGINE).
- Análisis de información y resultados.
- Análisis vulnerabilidades mediante NMAP NSE.
- Análisis vulnerabilidades mediante utilitarios independientes

5 Análisis de las vulnerabilidades

- Analizadores de vulnerabilidades (genéricos).
- Analizadores a nivel de aplicación (protocolos específicos).

6 Inseguridad en aplicaciones Web

- Vulnerabilidades Web - Introducción. OWASP TOP 10.
- Aplicaciones vulnerables para prácticas

7 Explotación de vulnerabilidades

- Código fuente de scripts en bases de datos públicas en Internet. (EXPLOIT DB)
- Usando metasploit framework.
- Password cracking

*Cada hora académica tiene una duración de 45 minutos

**Contenido referencial sujeto a cambios