Curso Especializado de **Ciberseguridad OFENSIVA**

Beneficios de capacitarse **online**

Tutor Personal

Conexión
desde cualquier dispositivo inteligente

Apoyo
personalizado y permanente

Ahorro de Costos.

Presentación:

El curso online de Ciberseguridad ofensiva, esta orientado a cubrir la demanda de profesionales experimentados en el área de seguridad. El curso no solo se encarga de instruir al participantes en técnicas de pruebas de pentetración y Ethical hacking, si no también tiene como objetivo adiestrarlo en las metodología para la ejecución de proyectos de consultoría en análisis de vulnerabilidades y pruebas de penetración como OSSTMM, OWASP, CVSS las cuales son reconocidas a nivel global.

Dirigido a:

Administradores de red, programadores, Auditores de Tecnologías de Información, Estudiantes de Informática, Sistemas, carreras afines.

Objetivos:

Utilizar las técnicas de los “hackers” cuando atacan servidores y clientes a través de Internet.

Tener el conocimiento necesario para realizar una prueba de penetración.

Utilizar en forma práctica las herramientas que se utilizan en un proceso de Ethical Hacking y conocer las metodologías OSSTMM y OWASP.

Preparar al participante en rendir los exámenes CPTE y CSWAE de Mile2.

Certificación:

Para todos los participantes que aprueben el 80% del curso personalizado, el CIDE entregara una certificación por 40 horas académicas de participación y aprobación.

Horario:

Sesiones mínimas de 04 horas o máximo de 06 horas.

De 14h00 a 18h00

Facilitador: Juan Oliva

Consultor de seguridad informática con mas de 14 años de experiencia en el campo, muy involucrado en proyectos de Ethical Hacking, análisis y explotación de vulnerabilidades, pruebas de ingeniería social, seguridad física, revisión de código, entre otras tareas de seguridad informática.

Ha ejecutado proyectos de Ethical Hacking para una variedad de empresas, en donde ha desarrollado proyectos para el estado peruano, así como para entidades privadas, nacionales y del extranjero.

Es instructor de cursos de Ethical Hacking y certificaciones como Linux Professional Institute, donde ha tenido oportunidad de realizar capacitaciones en el Perú, así como en el extranjero, Ponente de eventos nacionales e internacionales en España, México, Colombia, Ecuador, Chile, y en Perú.

Cuenta con certificaciones vigentes en Hacking y Linux como :

EC Council Certified | Ethical Hacker™ (CIEH)

Mile2 Certified) Penetration Testing Engineer (CPTE)

Mile2 Certified Secure Web Application Engineer (CSWAE)

Linux Professional Institute LPIC-1

Brainbench Certified Network Security (BNS)

Material a tener por participantes:

Máquinas Virtuales para ejercicios (Windows & Linux).

Diapositivas del Curso, Herramientas, Ejercicios, Laboratorios y Documentos de Referencia.

Requerimientos del alumno:

Conocimiento básico de Redes y programación.

Conocimiento de uso con VirtualBox y maquinas virtuales.

Conocimiento básico de Linux.

Material a tener por participantes:

Máquinas Virtuales para ejercicios (Windows & Linux).
Diapositivas del Curso, Herramientas, Ejercicios, Laboratorios y Documentos de Referencia.

Requerimientos del alumno:

Conocimiento básico de Redes y programación.
Conocimiento de uso con VirtualBox y maquinas virtuales.
Conocimiento básico de Linux.

Requerimiento de equipo:

PC/LAPTOP con capacidad para levantar al menos cuatro maquinas virtuales en simultaneo (512MB cada una)
Se recomienda equipos como mínimo procesador Intel I5 con 08 GB de RAM.
Software Oracle VirtualBox como plataforma de visualización.
Sistema operativo Windows 7 o 10 verificar que el Firewall y/o antivirus permitan la libre ejecución de maquinas virtuales y conectividad de red entre ellas en modo puente.
50 GB de espacio libre de disco duro para maquinas virtuales.

Temario

MODULO 1 – INTRODUCCION AL ETHICAL HACKING

• Introducción al Ethical Hacking , Tendencias Actuales. Dónde Apuntan los ataques hoy, Riesgos y Componentes Asociados. Nuevos Riesgos
• Metodologías de Penetration Testing - Ethical Hacking , Introducción a OSSTM, OWASP, CVSS.
• Como platear un proyecto y/o servicio de Ethical Hacking, documentación y formatos requeridos.

MODULO 2 – ETHICAL HACKING NETWORKING

• Footprint y reconocimiento con Google Hacking e Interrogación DNS .
• Escaneo de red redes con Nmap
• Enumeración de servicios
• Ataques de password craking a servicios
• CTF 1 : Obteniendo información del objetivo

MODULO 3 - EXPLOITS Y VULNERABILIDADES

• Trabajando con exploits
• Introducción a Metasploit como framework de ataque
• Ataques a sistemas operativos Windows
• Ataques del lado Cliente
• Creando ejecutables infectados (Virus) , para conseguir control de Windows.

MODULO 4 – ESCANEO DE VULNERABILIDADES

• Instalación y personalización de Nessus
• Escaneo de Vulnerabilidades avanzada con Nessus a nivel de Plataforma y aplicaciones
• Entendiendo reportes de Nesuss , detección de falsos positivos y falsos negativos
• CTF 2 : Detectando y explotando vulnerabilidades de un servidor

MODULO 5 - ETHICAL HACKING A APLICACIONES WEB

• Introductorio a vulnerabilidades web
• Uso de proxys de interceptación Burp Suite, ZAP Proxy
• Explotando vulnerabilidades, en PHP y .NET ASP
• Ataques a servidores Web con Sql Inyection
• Explotando vulnerabilidades XSS, LFI, RFI, Upload, SQLI POST, Evacion de Login, HTML inyection, Ataques de fuerza bruta contra formularios de autenticacion, Acceso inseguro de objetos.
• Ataques de robo de sesión o session hijacking
• Haciendo un defacement (defaceo) de una pagina web

MODULO 6 - ETHICAL HACKING DE API, SERVICIOS WEB Y MICROSERVICIOS

- Introductorio a los servicios web, SOAP, REST
- Ataques contra servicios web SOAP, SQL Inyection, WSDL Scanning, Web Service SAX Injection.
- Ataques contra API REST, divulgacion de información, Roptura de acceso, Inyecciones de SQL, devibilidad en token JSON, Mongo inyection, API google Hacking.
- Ataques contra microservicios en contenedores Docker

MODULO 7 - ETHICAL HACKING A APLICACIONES MOVILES

- Introductorio a las aplicaciones Moviles en Andrioid y iOS
- Instalación de emulador para aplicaciones Android
- Análisis, descarga y descompresión de APK
- Crear archivos .java y analisis de métodos de la aplicación
- Análisis de dexfiles
- Capturar credenciales mediante log de la aplicación
- Análisis de bases de datos SQLITE
- Análisis de almacenamiento externo
- Ataques de inyeccion de SQL
- Captura de paquetes con ZAP Proxy
- Análisis dinámico de aplicaciones móviles con Frida
- Envenenamiento de aplicaciones móviles con Metasploit

Modalidad: 100% online

en directo por la plataforma

ZOOM CLOUD MEETINGS

Fecha: 21,22, 23 y 24 de abril del 2020

Horarios: 14h00 a 18h00 PM

Inversión:
$20 Estudiantes
$40 Profesionales

Formas de Pago:
Transferencia Bancaria Banco Pichincha
Cta. Cte #2100146446 A nombre del Centro de Investigación
y Desarrollo Ecuador, CIDE S.A. - Ruc: 0992690305001

Inscripción:
1. Enviar el comprobante de transferencia bancaria al correo: marketing@cidecuador.org adjuntando sus datos personales (nombres completos, cedula, numero celular y correo)
2. Recibirá el correo de confirmación de su respectiva inscripción

CIDE

www.cidecuador.org **proyectocide**

Bryan Tello – 0996800630
Antonio Baque - 0996800656