CAPACITACIÓN

CERTIFICACIÓN HACKING ÉTICO POR EC-COUNCIL v9

CEH (CertifiedEthical Hacker) es la certificación oficial de **Hacking Ético** desde una perspectiva independiente de fabricantes. **El Hacker Ético** es la persona que lleva a cabo intentos de intrusión en redes y/o sistemas utilizando los mismos métodos que un **Hacker**. La diferencia más importante es que el **Hacker Ético** tiene autorización para realizar las pruebas sobre los sistemas que ataca. El objetivo de esta certificación es adquirir conocimientos prácticos sobre los sistemas actuales de seguridad para convertirse en un profesional del **hacking ético.**

Informática Integrada Internetworking es un centro de Entrenamiento Acreditado por **EC-Council®** en México en el que sus instructores oficiales son expertos en **Hacking Ético** y **Pentest** con más de 15 años de experiencia y del más alto nivel.

Este entrenamiento se lleva a cabo en un laboratorio extremadamente desafiante utilizando escenarios reales que enfrentan los profesionales en **Offensive Security** durante las pruebas de penetración en vivo.

Dirigido a: Gerentes y directores del área de seguridad de la información, especialistas en TI, auditores de seguridad, proveedores de Internet, administradores, gerentes de seguridad física y corporativa, profesionales de las áreas de computación, sistemas y comunicaciones que deseen actualizar sus conocimientos e implementar seguridad en sus centros de datos.

BENEFICIOS:

- Ofrecerá un panorama acerca de las vulnerabilidades halladas en los sistemas de información, lo cual puede anticiparse a estos ataques y prevenir muchos daños.
- Blindaran los recursos informáticos y telecomunicaciones de las organizaciones para soportar cualquier tipo de ataque un hacker externo o interno, evitando así contratiempos o daño a la infraestructura, o continuidad del negocio.
- Evitará que hackers maliciosos obtengan acceso a información sensible
- La certificación **CEH** aumenta tus oportunidades de empleo ya que las más empresas importantes lo solicitan.
- Estarás por encima de tus competidores

Informática Integrada Internetworking

PEARSON VUE-Authorized Test Center

TRAINING EC-Council PARTNER

Informatica Integrada Internetworking, SA de CV
Tel. (52-55) 5639-6517 y 5639-5715 Lada: 01-800-282-38 46 informes@informaticaintegrada.com.mx

Requisitos: Conocimientos básicos en sistemas operativos y redes

Duración: 48 Hrs.

Por qué estudiar con nosotros

- Somos una empresa especializada en **Seguridad TI** y **Pentest**
- Entrega de la documentación y manuales oficiales
- Se realizan prácticas en vivo y con escenarios reales
- Incluimos el **Voucher** de **Certificación Ethical Hacker**
- Realización del Examen nuestra instalaciones
- Certificación de validez internacional
- Somos un centro de **Certificación Oficial Pearson VUE®** y **EC-Council®**

INCLUYE:

- Instalaciones adecuadas
- Material y manuales de cursos
- Instructores Certificados
- **Voucher de Examen**
- Box lunch
- Servicio de cafetería continua
- Estacionamiento
- Registro **STPS**

Informatica Integrada Internetworking, SA de CV
Tel. (52-55) 5639-6517 y 5639-5715 Lada: 01-800-282-38 46 informes@informaticaintegrada.com.mx

TEMARIO:

Introducción al Hacking Ético

- Seguridad de la información
- Delitos en internet
- Amenazas y principios de defensa
- Conceptos de **Hacking**
- Tipos de ataque sobre un sistema
- Importancia de tener un **Ethical Hacking** en la empresa
- Habilidades de un **Hacker**
- Tipo de ataques
- ¿Qué es **Penetration testing**?
- Metodologías para realizar un **Pentesting**

Huellas digitales y reconocimiento

- **Footprinting**
- ¿Qué es **Footprinting**?
- Objetivos de **Footprinting**
- información que necesita un **hacker** para lanzar un ataque
- Buscando información de la compañía
- Herramientas **Footprinting** para realizar búsquedas
- Coleccionando de información de ubicación
- Obteniendo información de inteligencia competitiva
- **WHOIS Lookup** y extraer información de **DNS**
- Localizar rangos de red, **traceroute** y sitios web
- Extraer información de un sitio web
- Monitoreando actualizaciones web
- Seguimiento de comunicaciones de correo
- **Footprinting** usando técnicas de **Google Hacking®**
- Herramienta **Google Hacking®**
- **Pentesting Footprinting**

Redes y exploración

- Escaneando redes
- Tipos de escaneo
- Escaneo redes locales y direcciones IP
- Escaneo de puertos abiertos
- Escaneo de servidores
- Técnicas de evasión de **IDS**
- servicios de dudosa seguridad
- Comprobando sistemas activos con **ICMP Scanning**
- **Ping Sweep**, **Three-Way Handshake** y **TCP ags**
- **Hping2**, **Hping3**
- Técnicas de escaneo
- Técnicas de evasión de **IDS**

- Herramientas de fragmentación IP
- Uso de herramientas para escaneo
- **Nmapy NetScan. Proxier, SSH Tunneling**, etc.
- **Spoong IP address** y **Scanning Pentesting**

Enumeración

- Que es la enumeración
- Tipos de enumeración
- Enumeración de usuarios
- Enumeración de equipos
- Enumeración de recursos compartidos
- Enumeración **NetBIOS**, **SNMP**, **UNIX/Linux**, **LDAP**, **NTP**, **SMTP**, **DNS**
- Herramientas de enumeración y uso

Hackeo del sistema

- Objetivos del **Hackeo**
- Metodologías de **Hacking Ético**
- Metodología de **Hackeo CEH** (**CHM**)
- Etapas para el **Hackeo CEH**

Troyanos y Backdoors

- Troyanos
- Canales **Overty Covert**
- Tipos de troyanos
- Cómo trabajan los troyanos
- Indicaciones de ataques de troyanos
- Detección de troyanos
- Herramientas para detectar troyanos
- Anti-troyanos
- Evitar infección de troyanos
- **Backdoors** y contramedidas

Virus y gusanos

- Introducción a virus
- Ciclo de vida de un virus
- Indicaciones de ataque de virus
- ¿Cómo una máquina logra infectarse de virus?
- Tipos de virus y **Worms**
- Diferencia entre virus y **Worms**
- Analizando **Worms**
- Procedimiento para analizar malware
- Método para detectar **virus**
- Contramedidas para **virus** y **Worms**

Sniffers

- Conceptos de **Sniffers**
- Intercepción legal
- Cómo trabaja un **Sniffer**y sus amenazas
- Tipos de **Sniffers** y protocolos vulnerables a **Sniffing**
- Analizador de protocolos de hardware
- envenenamiento **MAC**
- envenenamiento **ARP**
- envenenamiento **DNS**
- Contramedidas contra **Sniffing**

Ingeniería social

- Ingeniería social
- fases en el ataque de la ingeniería social
- Tipos de ingeniería social
- Robo de identidad
- Tácticas de intrusión y estrategias para prevención
- Ingeniería social sobre sitios
- Riesgo de red social para redes corporativas

Denegación de servicios (DoS)

- Ataque de negación de **DoS**
- Técnicas de ataques **DoS**
- **Botnet** y Herramientas de ataque **DoS**
- Contramedidas **DoS/DDoS**
- Contramedidas en un ataque de **DDoS**
- Técnicas para defenderse contra **Botnets**
- pruebas de penetración para **DoS**

Sesión de secuestros (Hijacking)

- Sesión **Hijacking**
- Tipos de sesión **Hijacking**
- ¿Cómo predecir una sesión token?
- Diferentes tipos de ataques
- Número de secuencia y **TCP/IP Hijacking**
- Herramientas para **Hijacking**
- Contramedidas para H**ijacking**

Ataque a servidores Web

- Servidores Web
- Diferentes tipos de ataques web.
- Metodología en el ataque de un servidor web
- ataque a servidores web

- Contramedidas
- parches y herramientas de seguridad Web
- pruebas de penetración a servidores web

Ataque a aplicaciones Web

- Introducción a aplicaciones web
- Diferentes tipos de ataques
- Arquitectura de servicios web
- Analizando aplicaciones web
- Herramientas para hacking aplicaciones web
- Hacking a aplicaciones web
- Contramedidas en las aplicaciones web

Inyección SQL

- **SQL injection**
- Amenazas y ataques en **SQL injection**
- **HTTP** post request
- Detección de **SQL injection**
- **SQL injection Black Box Pen Testing**
- Tipos de **SQL injection**
- ¿Qué es **Blind SQL Injection**?
- Metodología en **SQL injection**
- Obtener información y enumerar columnas
- **Password grabbing** y características de diferentes **DBMSs**
- Herramientas para **SQL injection**, evadir **IDS**
- Contramedidas

Hackeo en redes inalámbricas

- Redes inalámbricas
- Tipos de redes inalámbricas
- Estándares de redes inalámbricas (**802.11 a,b,g**)
- Modos de autenticación con **Wi-Fi**
- Tipos de antenas
- Encriptación **WEP** y **WPA**
- Amenazas en redes inalámbricas
- Ataques a Access Point
- tipos de ataques
- Metodología **Wireless Hacking**
- Descubriendo **Wi-fi** usando **Wardriving**
- Analizando tráfico inalámbrico
- Herramientas para craquear **WEP/WPA** y **Wardriving**
- Herramientas de análisis, captura y monitoreo para **Wi-Fi**
- Contramedidas en redes inalámbricas
- auditando la seguridad en redes inalámbricas

Evadiendo IDs, Firewall y Honeypots

- Sistema de Detección de Intrusos
- Cómo detectar un intruso
- Tipos de **IDS**
- Herramientas de **IDS** y **Honeypot**
- Tipos de evasión
- Pasando sitios bloqueados usando direcciones IP en lugar de URL
- Detectando **Honeypots**, herramientas y contramedidas
- **Penetration Testing** para **IDS** y **Firewalls**

Desbordamiento Buffer (Buffer Overflow)

- Desbordamiento de **Buffer Overflow**
- Metodología **Buffer Overflow**
- Pasos en el desbordamiento de **buffer**
- Detectando desbordamiento de **buffer** en un programa
- Identificar el desbordamiento de **buffer**
- Detección del desbordamiento de **buffer**
- Herramientas de seguridad para el desbordamiento de **buffer**
- Contramedidas

Criptografía

- Criptografía
- Algoritmos de criptográficos
- **RSA (Rivest Shamir Adleman)**
- **RC4, RC5, RC6, Blowsh**
- **MD5** y **SHA**
- Herramientas para la criptografía
- **PKI**, firma digital y autoridad certificadora
- **SSL** y **TLS**
- Encriptación de discos y herramientas
- Ataques a la criptografía
- Herramientas de análisis criptográfico

Pruebas de Penetración

- Introducción a pruebas de penetración
- Evaluando la seguridad y vulnerabilidades
- Tipos de **penetration testing**
- técnicas comunes de **penetration testing**
- Usando información de DNS y direcciones IP
- Fases de **penetration testing**
- Metodología de **penetration testing**
- Tipos de **Pentest**
- Evaluación de la seguridad de aplicaciones
- Evaluación de la seguridad de la red

- Evaluación del acceso remoto e inalámbrico
- Evaluación de la seguridad telefónica
- Evaluación del filtrado de red