Certified Ethical Hacker | CEH | Versión 10

Referencia
JJS 550v10

Duración (horas)
40

Última actualización
5 junio 2018

Modalidades
Presencial, OpenClass®, a medida presencial

Examen
312-50

Certificación
Certified Ethical Hacker (CEH)

Introducción

El objetivo del curso es presentar a los asistentes los contenidos y habilidades necesarios para analizar la seguridad de los sistemas de seguridad. El curso cubrirá los conceptos de escaneo, pruebas, hacking y aseguración de sistemas. Se analizarán los diferentes problemas, amenazas y vulnerabilidades de los sistemas de información como detección, creación de políticas, análisis, control de acceso, etc.

Objetivos

Al finalizar este curso los alumnos podrán:

- Escalar privilegios
- Asegurar sistemas
- Detectar intrusiones
- Escanear sistemas en búsqueda de amenazas o vulnerabilidades
- Aplicar técnicas de intrusión

Perfil de los alumnos

- Profesionales TI
- Responsables de seguridad
- Auditores
- Administradores de sistemas

Requisitos previos

- Amplio conocimiento de TCP/IP
- Background de sistemas de información y de seguridad
- Al menos 2 años de experiencia en seguridad de la información
- Conocimiento medio-avanzado de Windows y Linux

Metodología

Curso presencial, activo y participativo. El docente introducirá los contenidos haciendo uso del método demostrativo, los participantes asimilarán los conocimientos mediante las prácticas de aplicación real.

Certificación

Evaluación continua en base a las actividades realizadas en grupo y/o individualmente. El formador proporcionará feedback de forma continuada/al final de las actividades/individualmente a cada participante.

Las condiciones de los servicios adicionales de Certificación están sujetos a los términos del propietario de la licencia o de la entidad certificadora autorizada.

Profesorado

Contamos con un equipo de instructores altamente cualificados que combinan la actividad formativa con el desarrollo de su actividad profesional como expertos en el campo de las TIC. Profesionales certificados por los principales fabricantes del sector capaces de transferir de forma amena y entendedora los conceptos técnicos más abstractos.

Documentación

Para poder seguir el curso los alumnos recibirán una copia de la documentación de EC-Council.

Esa documentación se complementa con apartados de referencias adicionales bien comprobadas, para que el alumno pueda extender esta formación en su trabajo real.

Contenidos

- **Introducción al Ethical Hacking**
- Visión general de la Seguridad de la Información
- Amenazas y ataques a la Seguridad de la Información
- Conceptos de Hacking
- Tipos de ataques
- Controles de la Seguridad de la Información

- **Footprinting y reconocimiento**
- Conceptos de footprinting
- Amenazas de footprinting
- Metodología de footprinting
- Herramientas de footprinting
- Medidas de footprinting
- Pruebas de penetración de footprinting

- **Escaneo de redes**
- Conceptos de escaneo de redes
- Herramientas de escaneo
- Técnicas de escaneo
- Pen Testing

- **Enumeración**
- Conceptos de enumeración
- NetBIOS
- SNMP
- LDAP
- NTP
- SMTP y DNS
- Métricas de enumeración / SMB
- Pruebas de penetración de enumeración

- **Análisis de vulnerabilidades**
- Conceptos de evaluación de vulnerabilidades
- Soluciones de evaluación de vulnerabilidades
- Sistemas de scoring de vulnerabilidades
- Herramientas de evaluación de vulnerabilidades
- Informes de evaluación de vulnerabilidades

- **Hacking de sistemas**

- Información previa a la fase de hacking
- Objetivos del hacking de sistemas
- Metodología de hacking CEH (CHM)
- Pasos del hacking de sistemas

- **Amenazas de malware**
- Introducción al malware
- Conceptos y tipos de troyanos
- Conceptos de virus y gusanos
- Ingeniería inversa de malware
- Detección de malware
- Métricas
- Software anti malware
- Pruebas de penetración para troyanos y puertas traseras

- **Sniffing**

- Conceptos de sniffing
- Ataques MAC
- Ataques DHCP
- Envenenamiento ARP
- Ataques por spoofing
- Envenenamiento DNS
- Herramientas de sniffing
- Métricas
- Pruebas de penetración de sniffing

- **Ingeniería social**
- Conceptos de ingeniería social
- Técnicas de ingeniería social
- Impersonalización en redes sociales
- Robo de identidades
- Métricas de ingeniería social
- Pruebas de penetración de ingeniería social

- **Denegación de servicio (DoS)**
- Conceptos DoS / DDoS
- Técnicas de ataque DoS
- Botnet
- Caso de estudio de DDoS
- Métricas
- Herramientas de protección DoS / DDoS
- Pruebas de penetración de ataque por Denegación de Servicio (DoS)

- **Hijacking de sesiones**
- Conceptos de hijacking de sesiones
- Hijacking de sesión a nivel de red
- Herramientas de hijacking de sesión
- Métricas
- Pruebas de penetración de hijacking de sesión

- **Evasión de IDS, Firewalls y Honeypots**
- Conceptos de IDS, Firewalls y Honeypots
- Sistemas IDS, Firewalls y Honeypots
- Evitar IDS
- Evitar Firewalls
- Detectar Honeypots
- Herramientas de evasión de Firewalls
- Métricas
- Pruebas de penetración

- **Hacking de servidores Web**
- Conceptos de servidores Web
- Ataques a servidores Web
- Metodología de ataque
- Herramientas de ataque a servidores Web
- Métricas
- Gestión de parches
- Herramientas de seguridad de servidores Web
- Pruebas de penetración a servidores Web

- **Hacking de aplicaciones Web**
- Conceptos de aplicaciones Web
- Amenazas de las aplicaciones Web
- Metodología de hacking de aplicaciones Web
- Herramientas de hacking de aplicaciones Web
- Métricas
- Herramientas de seguridad
- Pruebas de penetración a aplicaciones Web

- **Inyección SQL**
- Conceptos de inyección SQL
- Pruebas para inyección SQL
- Tipos de inyección SQL
- Falsear la inyección SQL
- Metodología de inyección SQL
- Inyección SQL avanzada
- Herramientas de inyección SQL
- Técnicas de evasión
- Métricas

- **Hacking de redes inalámbricas (Wireless)**
- Conceptos de Wireless
- Cifrado Wireless
- Amenazas Wireless
- Metodología de hacking Wireless
- Herramientas de hacking Wireless
- Hacking Bluetooth
- Métricas
- Herramientas de seguridad Wireless
- Pruebas de penetración Wi-Fi

- **Hacking de plataformas móviles**
- Vectores de ataque a plataformas móviles
- Hacking de Android OS
- Hacking de iOS

- Spyware móvil
- Gestión de dispositivos móviles (MDM)
- Líneas guía y herramientas de seguridad móvil
- Pruebas de penetración móvil

- **Hacking de IoT**
- Conceptos de IoT
- Ataques IoT
- Metodología de hacking de IoT
- Herramientas de hacking de IoT
- Contramedidas
- Pen Testing de IoT

- **Cloud Computing**
- Conceptos de Cloud Computing
- Amenazas del Cloud Computing
- Ataques al Cloud Computing
- Seguridad en Cloud
- Herramientas de seguridad en Cloud
- Pruebas de penetración en Cloud

- **Criptografía**
- Conceptos de Criptografía
- Algoritmos de cifrado
- Herramientas criptográficas
- Infraestructura de Clave Pública (PKI)
- Cifrado de e-mail
- Cifrado de disco
- Criptoanálisis
- Herramientas de criptoanálisis

Acreditación

Se emitirá Certificado de Asistencia sólo a los alumnos con una asistencia superior al 75% y Diploma aprovechamiento si superan también la prueba de evaluación.