
cybertrust
INSPIRANDO CONFIANZA
EC-Council
C|EH™
Certified Ethical Hacker

Certified Ethical Hacker (C | EH v10)

El programa Certified Ethical Hacker (C | EH v10) es un programa de capacitación en hacking ético confiable y respetado que cualquier profesional de seguridad de la información necesitará en su curriculum.

Desde su creación en 2003, Certified Ethical Hacker ha sido la elección absoluta de la industria a nivel mundial. Es una certificación respetada en la industria y está catalogada como una certificación de referencia en la Directiva 8570 del Departamento de Defensa de los Estados Unidos. El examen C | EH cumple con ANSI 17024 y agrega credibilidad y valor a los miembros que lo poseen.

C | EH se utiliza como estándar de contratación y es una certificación esencial solicitada por muchas de las organizaciones de Fortune 500, gobiernos, prácticas de seguridad y ciberseguridad un elemento básico en educación en muchos de los programas de grado más destacados en las principales universidades de todo el mundo.
Cientos de miles de profesionales de InfoSec y también Career Starters han desafiado el examen y, para los que aprobaron, casi todos tienen un empleo remunerado con carreras exitosas, pero el panorama está cambiando. La ciberseguridad como profesión está evolucionando, la barrera de entrada está en aumento, la demanda de profesionales especializados continúa creciendo se está perfeccionando y exigiendo un mayor nivel de habilidad
.

¡EC-Council vuelve a subir la barrera para los programas de formación y certificación de hacking ético con el nuevo C | EH v10!

Este curso, en su décima iteración, se actualiza para proporcionarle las herramientas y técnicas utilizadas por los piratas informáticos y los profesionales de la seguridad de la información para entrar en cualquier sistema informático. Este curso lo sumergirá en una "Mentalidad Hacker" para enseñarle a pensar como un hacker y defenderse mejor contra futuros ataques. Usted se posicionó en un entorno de capacitación práctica que emplea un proceso sistemático de hacking ético.
Estás constantemente expuesto a técnicas creativas para lograr una postura de seguridad de la información óptima en la organización objetivo; ¡Haciéndolo! Aprenderá a escanear, probar, piratear y proteger sistemas de destino. El curso cubre las Cinco fases de hacking ético, el buceo en el reconocimiento, la obtención de acceso, la enumeración, el mantenimiento del acceso y la cobertura de sus pistas.
Las herramientas y técnicas en cada una de estas cinco fases se proporcionan en detalle en un enfoque enciclopédico y absolutamente ningún otro programa le ofrece la variedad de recursos de aprendizaje, laboratorios, herramientas y técnicas que el programa C | EH v10.

C|EH Certified Ethical Hacker

El examen C | EH cumple con ANSI, lo que le otorga el respeto y la confianza de los empleadores a nivel mundial. Hoy en día, puedes encontrar profesionales de credenciales de C | EH en más de 145 países que trabajan con algunas de las corporaciones más grandes y mejores de todos los sectores, incluidos el gobierno, el ejército, las finanzas, la salud, la energía, el transporte y muchos más.

El C | EH (Práctico) es un examen práctico de 6 horas construido según especificaciones exactas por expertos en la materia en el campo EH. Los profesionales que poseen la credencial C | EH podrán presentarse para el examen que pondrá a prueba sus límites para desenterrar las vulnerabilidades en los principales sistemas operativos, bases de datos y redes. Para aquellos que cumplen y superan el nivel de habilidades establecido, obtendrán la nueva certificación requerida por la industria: la certificación C | EH (Práctica).

C | EH (Práctico) está disponible con supervisión en línea, con instalaciones remotas en todo el mundo.

El beneficio combinado de un examen práctico que se supervisa completamente en cualquier lugar del mundo proporcionará a las organizaciones una credencial validada y confiable cuando empleen profesionales de ciberseguridad. Con su disponibilidad global, las organizaciones ahora pueden entrenar, probar e implementar rápidamente una fuerza de trabajo preparada para el ciberespacio de manera efectiva.

El examen C | EH cumple con ANSI, lo que le otorga el respeto y la confianza de los empleadores a nivel mundial. Hoy en día, puedes encontrar profesionales de credenciales de C | EH en más de 145 países que trabajan con algunas de las corporaciones más grandes y mejores de todos los sectores, incluidos el gobierno, el ejército, las finanzas, la salud, la energía, el transporte y muchos más. C | EH (ANSI) C | EH (PRÁCTICA)

Detalles del E x a m e n

- Título del examen: Hacker ético certificado (práctico)
- Número de desafíos prácticos: 20
- Duración: 6 horas
- Disponibilidad: Aspen-iLabs
- Formato de prueba: iLabs Cyber Range
- Calificación de aprobación: 70%
- Título del examen: Certified Ethical Hacker (ANSI)
- Código de examen: 312-50 (ECC EXAM), 312-50 (VUE)
- Cantidad de preguntas: 125
- Duración: 4 horas
- Disponibilidad: ECCEXAM / VUE
- Formato de prueba: opción múltiple
- Calificación de aprobación: consulte https://cert.eccouncil.org/faq.html

El C | EH (Práctico) es un examen práctico de 6 horas construido según especificaciones exactas por expertos en la materia en el campo EH. Los profesionales que poseen la credencial C | EH podrán presentarse para el examen que pondrá a prueba sus límites para desenterrar las vulnerabilidades en los principales sistemas operativos, bases de datos y redes. Para aquellos que cumplen y superan el nivel de habilidades establecido, obtendrán la nueva certificación requerida por la industria: la certificación C | EH (Práctica).

C | EH (Práctico) está disponible con supervisión en línea, con instalaciones remotas en todo el mundo.
El beneficio combinado de un examen práctico que se supervisa completamente en cualquier lugar del mundo proporcionará a las organizaciones una credencial validada y confiable cuando empleen profesionales de ciberseguridad. Con su disponibilidad global, las organizaciones ahora pueden entrenar, probar e implementar rápidamente una fuerza de trabajo preparada para el ciberespacio de manera efectiva.

Criterio de Elegibilidad

Ser un miembro de CEH al día (su tarifa de solicitud de USD 100 no se aplicará);

o Tener un mínimo de 3 años de experiencia laboral en el dominio de InfoSec (deberá abonar USD 100 como tarifa de solicitud no reembolsable);

o tener otras certificaciones equivalentes de la industria, como OSCP o GPEN cert (tendrá que pagar USD 100 como una tarifa de solicitud no reembolsable).

Los 10 Principales Componentes Críticos de C | EH v10

Cumplimiento del 100% de NICE 2.0 Framework C | EH v10 se asigna en un 100% al área de especialización Protect and Defend de NICE framework

Inclusión del nuevo análisis de vulnerabilidad de módulos
Aprenda a realizar análisis de vulnerabilidad para identificar los vacíos de seguridad en el objetivo o la red de la organización, infraestructura de comunicación y sistemas finales.

Este módulo cubre el ciclo de vida de la gestión de vulnerabilidades y diversos enfoques y herramientas utilizado para realizar la evaluación de vulnerabilidad.

Hacking de IoT
Comprenda las posibles amenazas a las plataformas de IoT y aprenda cómo defender los dispositivos de IoT de forma segura.

Concéntrese en los vectores emergentes de ataque (por ejemplo, Cloud, AI, ML, etc.) C | EH proporciona información sobre las amenazas informáticas en la nube y los ataques informáticos en la nube.

Analiza la seguridad informática en la nube y las herramientas necesarias.

Proporciona una visión general de los pasos de prueba que un hacker ético debe seguir para realizar una segura evaluación del entorno de la nube.

La inteligencia artificial (IA) es una solución emergente utilizada en la defensa de redes contra varios ataques que un análisis antivirus no puede detectar. Aprenda cómo se puede implementar esto a través del curso C | EH.

Desafíos de hacking al final de cada módulo
Los desafíos al final de cada módulo garantizan que pueda practicar lo que ha aprendido.

Ayudan a los estudiantes a comprender cómo el conocimiento puede transformarse en habilidades y pueden ser utilizado para resolver problemas de la vida real.

C|EH Certified Ethical Hacker

Cobertura del último Malware
El curso se actualiza para incluir el último ransomware, en la industria financiera ¡malware, botnets IoT, malwares de Android y más!

Inclusión de un proceso completo de análisis de malware. Descubra y aprenda a utilizar el malware de ingeniería inversa para determinar el origen, funcionalidad y el impacto potencial de un malware.

Al realizar análisis de malware, la información detallada sobre el malware se puede extraer, analizar y esto es una habilidad crucial de un hacker ético.

Programa práctico mas del 40 por ciento del tiempo de clase está dedicado al aprendizaje de habilidades prácticas y esto se logra a través de los laboratorios del Consejo de la C|EC
C | EH Le proporciona a los estudiantes una experiencia práctica de la últimas técnicas, metodologías, herramientas, pruebas de pentesting etc.

C | EH viene integrado con los laboratorios para enfatizar los objetivos de aprendizaje. También proporciona laboratorios adicionales que los estudiantes pueden practicar después del entrenamiento en su propio tiempo, a través de la Plataforma iLabs de EC-Council que los estudiantes pueden comprar por separado.

Entorno de laboratorio simula un entorno en tiempo real El entorno de laboratorio C | EH v10 consta de los últimos sistemas operativos, incluido Windows

Servidor 2016 y Windows 10 configurados con controlador de dominio, firewalls y aplicaciones web vulnerables para perfeccionar las habilidades de ataque.

Cubre las últimas herramientas de ataque (basadas en Windows, MAC, Linux y móvil) El curso C | EH v10 incluye una biblioteca de herramientas que los profesionales de seguridad y pentesters requieren para descubrir vulnerabilidades en diferentes plataformas de operación.

Esto proporciona una opción más amplia para los estudiantes que cualquier otro programa en el mercado.

Acreditación ANSI La acreditación ANSI significa que el titular de la certificación ha completado una curso de estudio diseñado específicamente para cumplir con los predefinidos de la industria.

Temario de CURSO

1. Introducción al Hacking ético
2. Footprinting y Reconocimiento de objetivos
3. Escaneo de redes
4. Enumeración
5. Análisis de vulnerabilidad
6. Amenazas de Malware
7. Sniffing
8. Ingeniería social
9. Denegación de servicio
10. Secuestro de sesión
11. Evadiendo IDS, firewalls y Honeypots
12. Hacking o Servidores web
13. Hacking de aplicaciones web
14. Inyección SQL
14. Hacking Redes inalámbricas
15. Hacking Plataformas móviles
16. IoT Hacking
17. Cloud Security
18. Criptografía

CEH Certified Ethical Hacker

¿Qué aprenderás?

1. Problemas clave que afectan el mundo de la seguridad de la información, el proceso de gestión de incidentes y las pruebas de penetración.
2. Varios tipos de huella, herramientas de huella y contramedidas.
3. Técnicas de escaneo en red y contramedidas de escaneo.
4. Técnicas de enumeración y contramedidas de enumeración.
5. Metodología de Pentesting del sistema, steganography, ataques de estegoanalisis y pistas de cobertura.
6. Diferentes tipos de troyanos, análisis de troyanos y contramedidas
7.Análisis de virus, gusanos informáticos, procedimiento de análisis de malware y contramedidas.
8. Técnicas de detección de paquetes y cómo defenderse contra el sniffing.
9. Técnicas de ingeniería social, identificar robos y contramedidas de ingeniería social.
10. Técnicas de ataque DoS / DDoS, botnets, herramientas de ataque DDoS y contramedidas DoS / DDoS.
11. Técnicas y contramedidas para el secuestro de la sesión.
12. Diferentes tipos de ataques al servidor web, metodología de ataque y contramedidas.
13. Diferentes tipos de ataques a aplicaciones web, metodología de pirateo de aplicaciones web y contramedidas.
14. Ataques de inyección SQL y herramientas de detección de inyección.
15. Cifrado inalámbrico, metodología de piratería inalámbrica, herramientas de piratería inalámbrica y herramientas de seguridad Wi-Fi.
16. Vector de ataque de la plataforma móvil, vulnerabilidades de Android, directrices de seguridad móvil y herramientas.
17. Cortafuegos, IDS y técnicas de evasión de honeypot, herramientas de evasión y contramedidas.
18. Diversos conceptos, amenazas, ataques y herramientas y técnicas de seguridad en la nube.
19. Diferentes tipos de ciphers de criptografía, Public Key Infrastructure (PKI), ataques de criptografía y herramientas de criptoanálisis.
20. Varios tipos de pruebas de penetración, auditoría de seguridad, evaluación de vulnerabilidad y hoja de ruta de pruebas de penetración.
21. Realice un análisis de vulnerabilidad para identificar los agujeros de seguridad en la red de la organización objetivo, la infraestructura de comunicación y los sistemas finales.
22. Diferentes amenazas para plataformas IoT y aprenda cómo defender dispositivos IoT de forma segura.

www.cybertrust.cl

Av. Apoquindo 4775, Piso 3 - Las Condes, Santiago de Chile. Teléfono: +562 3224 3551 | +562 3224 3552 Email: contacto@cybertrust.cl