EC-Council

The All-New

C|EH® v12

Certified Ethical Hacker

1 LEARN

2 CERTIFY

3 ENGAGE

4 COMPETE

Attain the World's No.1 Credential in Ethical Hacking

Construye tu carrera con la certificación de ciberseguridad más demandada en el mundo:

SÉ UN HACKER ÉTICO CERTIFICADO

Certificación de Hacking Ético No. 1 del Mundo durante 20 Años

Clasificado #1
En Hacking Ético
Certificaciones por ZDNet

Clasificado como una de las 10 mejores certificaciones de ciberseguridad

C|EH®Rangos 4el
Entre las 50 principales certificaciones de ciberseguridad

¿Quién es un hacker ético certificado?

Un hacker ético certificado es un especialista que generalmente trabaja en un entorno de equipo rojo, enfocado en atacar sistemas informáticos y obtener acceso a redes, aplicaciones, bases de datos y otros datos críticos en sistemas seguros. CA|EH® comprende las estrategias de ataque, el uso de vectores de ataque creativos e imita las habilidades, la creatividad de los piratas informáticos malintencionados. A diferencia de los piratas informáticos y los actores maliciosos, los piratas informáticos éticos certificados operan con el permiso de los propietarios del sistema y toman todas las precauciones para garantizar que los resultados permanezcan confidenciales. Los investigadores de "bug bounty" son hackers éticos expertos que usan sus habilidades de ataque para descubrir vulnerabilidades en los sistemas.

¿Qué es C|EH?®v12?

El Certified Ethical Hacker se ha endurecido en batalla durante los últimos 20 años, creando cientos de miles de Certified Ethical Hackers empleados por las principales empresas, militares y gobiernos de todo el mundo.

En su 12.ª versión, Certified Ethical Hacker brinda capacitación integral, laboratorios de aprendizaje práctico,rangos cibernéticos de práctica para el compromiso, evaluaciones de certificación, competencias cibernéticas y oportunidades para el aprendizaje continuo en un programa integral seleccionado a través de nuestro nuevo marco de aprendizaje: 1. Aprende 2. Certificar 3. Participar 4. Competir.

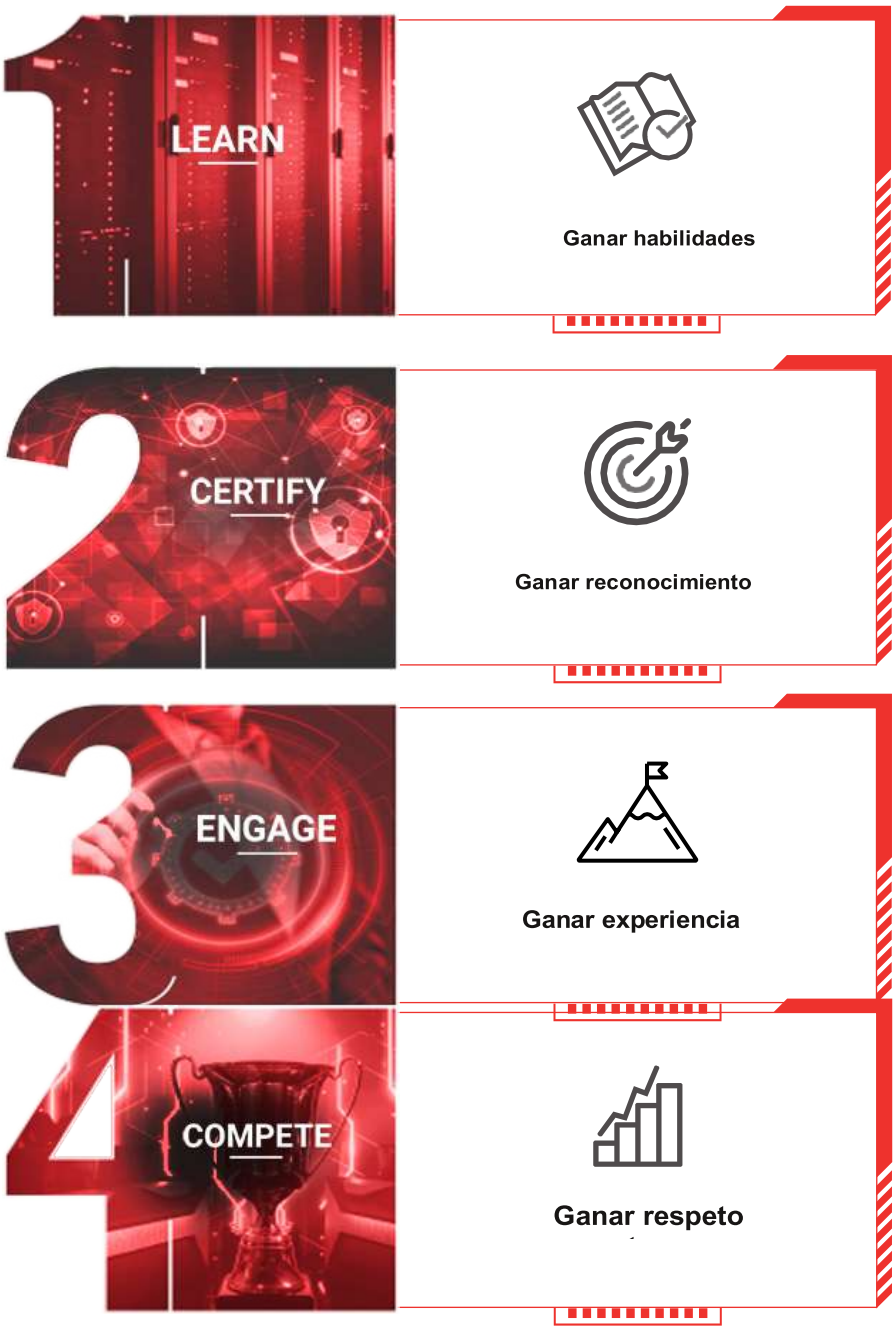
El C|EH v12 también equipa a los aspirantes a profesionales de la seguridad cibernética con las tácticas, técnicas y procedimientos (TTP) para crear piratas informáticos éticos que puedan descubrir debilidades en casi cualquier tipo de sistema de destino antes que los ciberdelincuentes.

Novedades en el C|EH ®v12

APRENDE | CERTIFICATE | COMBATE | COMPITE

El C|EH®v12 es un programa de capacitación especializado y único para enseñarle todo necesita saber sobre piratería ética con capacitación práctica, laboratorios, evaluación, un compromisosimulado (práctica) y competencia de piratería global. Manténgase al tanto del juego con el
habilidades más demandadas requeridas para tener éxito en el campo de la ciberseguridad.

Domina habilidades de hacking ético que van más allá de la certificación.



El nuevo aprendizaje framework cubre no sólo una amplia programa de entrenamiento para el exámen de certificación sino también la industria más robusta y profunda, laboratorio práctico con un campo de práctica y experiencia.

Entra en el Hackerverso ™Con el C|EH®v12

Mejore su carrera de piratería ética

1 LEARN

- 5 días de entrenamiento
- 20 módulos
- Más de 3000 páginas del manual del estudiante
- Más de 1900 páginas de manual de laboratorio
- Más de 200 laboratorios prácticos con banderas de competencia
- Más de 3500 herramientas de piratería
  - Aprende a hackear múltiples sistemas operativos (Windows 11, servidores Windows, Linux, Ubuntu, Android)
- Marco de ataque MITRE
- Modelo de diamante de análisis de intrusión
- Técnicas para establecer la persistencia
- Evadir NAC y seguridad de punto final
- Comprender el modelo de computación de niebla, borde y cuadrícula

2 CERTIFY

C|EH®ANSI

- 125 preguntas de opción múltiple
- 4 horas

C|EH®Práctico

- Examen práctico de 6 horas
- 20 preguntas basadas en escenarios

3 ENGAGE

- Llevar a cabo una tarea de piratería ética del mundo real
- Aplicar las 5 fases
  - Reconocimiento
  - Escaneo
  - Ganando acceso
  - Mantenimiento del acceso
  - Cubriendo tus huellas

4 COMPETE

- Nuevos desafíos cada mes
- Competición de 4 horas
- Compite con tus compañeros de todo el mundo
- Ábrete camino hasta la cima dela clasificación
- Ganar reconocimiento
- Los desafíos incluyen:
  - Las 10 principales amenazas deaplicaciones web de OWASP
  - Vectores
  - Secuestro de datos/ Análisis de malware
  - Desactualizado/sin parchear Software
  - Piratería del sistema y escalada de privilegios
  - Aplicación web Hackeo y Pluma Pruebas
  - Ataque en la nube/Hackeo
  - y muchos más...

El C|EH®El programa de capacitación v12 incluye 20 módulos que cubren varias tecnologías, tácticas y procedimientos que brindan a los posibles piratas informáticos éticos el conocimiento básico necesario para prosperar en la ciberseguridad. Entregado a través de un plan de capacitación cuidadosamente curado que generalmente abarca cinco días, la 12.ª versión del C|EH®continúa evolucionando para mantenerse al día con los últimos sistemas operativos, exploits, herramientas y técnicas. Los conceptos cubiertos en el programa de capacitación se dividen 50/50 entre capacitación basada en el conocimiento y aplicación práctica a través de nuestra gama cibernética. Cada táctica discutida en la capacitación está respaldada por laboratorios paso a paso realizados en un entorno virtualizado con objetivos en vivo, herramientas vivas y sistemas vulnerables. A través de nuestra tecnología de laboratorio, cada participante tendrá una práctica integral para aprender y aplicar su conocimiento".

20 MÓDULOS ACTUALIZADOS

3000+ PÁGINAS DEL MANUAL DE ESTUDIANTE

Esquema del curso

20 módulos que lo ayudan a dominar los fundamentos de la piratería ética y prepararse para tomar el examen de certificación C|EH

Módulo 01

Introducción al Hacking Ético

Cubre los fundamentos de los problemas clave en el mundo de la seguridad de la información, incluidoslos conceptos básicos de la piratería ética, los controles de seguridad de la información, las leyes relevantes y los procedimientos estándar.

Módulo 02

Pie de impresión y reconocimiento

Aprenda a utilizar las últimas técnicas y herramientas para realizar huellas yreconocimiento, una fase crítica previa al ataque del proceso de piratería ética.

Módulo 03

Escaneo de redes

Aprenda diferentes técnicas de escaneo de red y contramedidas.

Módulo 04

Enumeración

Aprenda varias técnicas de enumeración, como el protocolo de puerta de enlace fronteriza (BGP) y las vulnerabilidades de uso compartido de archivos de red (NFS), y las contramedidas asociadas.

Módulo 05

Análisis de vulnerabilidad

Aprenda a identificar lagunas de seguridad en la red, la infraestructura de comunicación y los sistemas finales de una organización objetivo. Diferentes tipos deevaluación de vulnerabilidad y herramientas de evaluación de vulnerabilidad.

Módulo 06

Hackeo del sistema

Conozca las diversas metodologías de piratería de sistemas, incluida la esteganografía, los ataques de esteganálisis y las pistas de cobertura, que se utilizan para descubrir las vulnerabilidades del sistema y la red.

Módulo 07

Amenazas de malware

Aprenda diferentes tipos de malware (troyanos, virus, gusanos, etc.), APT y malware sin archivos, procedimiento de análisis de malware y contramedidas de malware.

Módulo 08

Detección

Obtenga información sobre las técnicas de detección de paquetes y cómo usarlas para descubrir vulnerabilidades de red, así como contramedidas para defenderse de los ataques de detección.

Módulo 09

Ingeniería social

Aprenda conceptos y técnicas de ingeniería social, incluido cómo identificar intentos de robo, auditar vulnerabilidades a nivel humano y sugerir contramedidas de ingeniería social.

Módulo 10

Negación de servicio

Conozca las diferentes técnicas de ataque de denegación de servicio (DoS) y DoS distribuido (DDoS), así como las herramientas utilizadas para auditar un objetivo, diseñar contramedidas y protecciones DoS y DDoS.

Módulo 11

Secuestro de sesión

Comprender las diversas técnicas de secuestro de sesiones utilizadas para descubrir la gestión de sesiones, la autenticación, la autorización y las debilidadescriptográficas a nivel de red y las contramedidas asociadas.

Módulo 12

Evadir IDS, Firewalls y Honeypots

Conozca el firewall, el sistema de detección de intrusos (IDS) y las técnicas de evasión de trampas trampa; las herramientas utilizadas para auditar un perímetro de red en busca de debilidades; y contramedidas.

Módulo 13

Hackear servidores web

Obtenga información sobre los ataques a servidores web, incluida una metodología de ataque integral utilizada para auditar las vulnerabilidades en las infraestructuras de los servidores web y las contramedidas.

Módulo 14

Hackear aplicaciones web

Obtenga información sobre los ataques a aplicaciones web, incluida una metodología integral de piratería de aplicaciones web que se utiliza para auditar las vulnerabilidadesen las aplicaciones web y las contramedidas.

Módulo 15

Inyección SQL

Obtenga información sobre los ataques de inyección SQL, las técnicas de evasión y las contramedidas de inyección SQL.

Módulo 16

Hackear redes inalámbricas

Comprender los diferentes tipos de tecnologías inalámbricas, incluidos el cifrado, las amenazas, las metodologías de piratería, las herramientas de piratería, las herramientasde seguridad de Wi-Fi y las contramedidas.

Módulo 17

Hackear plataformas móviles

Aprenda el vector de ataque de la plataforma móvil, la piratería de Android e iOS, la administración dedispositivos móviles, las pautas de seguridad móvil y las herramientas de seguridad.

Módulo 18

Hackeo de IoT

Aprenda diferentes tipos de ataques de IoT y OT, metodología de piratería,herramientas de piratería y contramedidas.

Módulo 19

Computación en la nube

Aprenda diferentes conceptos de computación en la nube, como tecnologías de contenedores y computación sin servidor, varias amenazas de computación en la nube, ataques, metodología de piratería y técnicas y herramientas de seguridad en la nube.

Módulo 20

Criptografía

Obtenga información sobre algoritmos de encriptación, herramientas de criptografía, infraestructurade clave pública (PKI), encriptación de correo electrónico, encriptación de disco, ataques de criptografía y herramientas de criptoanálisis.

LAS MANOS EN

LABORATORIOS DE APRENDIZAJE

Con más de 220 laboratorios prácticos realizados en nuestro entorno de rango cibernético, tendrá la oportunidad de practicar cada objetivo de aprendizaje en máquinas en vivo y objetivos vulnerables en el curso. Precargado conmás de 3500 herramientas de piratería y varios sistemas operativos, obtendrá una exposición y experiencia práctica sin precedentes con las herramientas de seguridad más comunes, las vulnerabilidades más recientes y los sistemas operativos ampliamente utilizados en la industria. Nuestra gama es accesible desde la web, lo que facilita el aprendizaje y la práctica desde cualquier lugar.

Qué está cubierto:

100%virtualización para una experiencia deaprendizaje completa

Después de iniciar sesión, tendrá acceso completo a objetivos preconfigurados, redes y las herramientas de ataque necesarias para explotarlos:

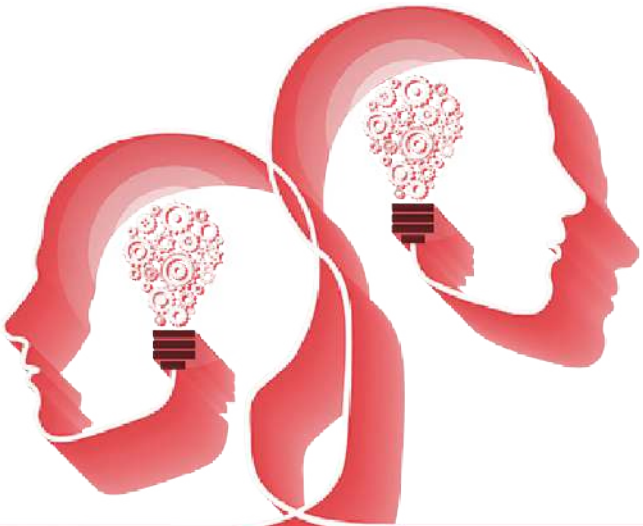
- Sitios web vulnerables preconfigurados
- Sistemas operativos vulnerables y sin parches
- Entornos completamente conectados en red
- Más de 3500 herramientas de piratería
- ¡Y mucho más!

Amplia gama de plataformas de destino para perfeccionar sus habilidades

519 técnicas de ataque

Indicadores orientados a objetivos para el pensamiento crítico y la evaluación del conocimiento aplicada

Gama cibernética basada en la nube



2 CERTIFY

Demuestre sus destrezas y habilidades con exámenes prácticos en línea

El hacker ético certificado con la credencial es reconocida globalmente como el estándar de la industria para evaluar la comprensión de la piratería ética y las pruebas de seguridad. Como examen acreditado por ANSI 17024, el examen supervisado de 150 preguntas y 4 horas es reconocido en todo el mundo como la certificación de seguridad cibernética táctica original y más confiable para piratas informáticos éticos. Los dominios de certificación se examinan cuidadosamente a través de profesionales de la industria, lo que garantiza que la certificación coincida con los requisitos actuales de la industria; este examen se somete a evaluaciones y ajustes psicométricos regulares para garantizar una medida justa y precisa del conocimiento del candidato en el dominio de la piratería ética.

Examen de conocimientos + **Examen de habilidades**

Knowledge		Skills/Abilities		Your Proof!
C | EH v12 Certified Ethical Hacker	+	C | EH ETHICAL HACKER PRACTICAL	=	C | EH Certified Ethical Hacker MASTER
4 horas Examen de opción múltiple		6 horas 20 desafíos prácticos		Alcanzar ¡Maestría!

Hacker Ético Certificado (C|EH)®) Certificación

El C|EH El examen , es un examen de 4 horas con 125 preguntas de opción múltiple. ¡Este examen basado en conocimientos pondrá a prueba sus habilidades en amenazas a la seguridad de la información y vectores de ataque, detección de ataques, prevención de ataques, procedimientos, metodologías y más!
Acceda a nuestro modelo de examen para C|EH®

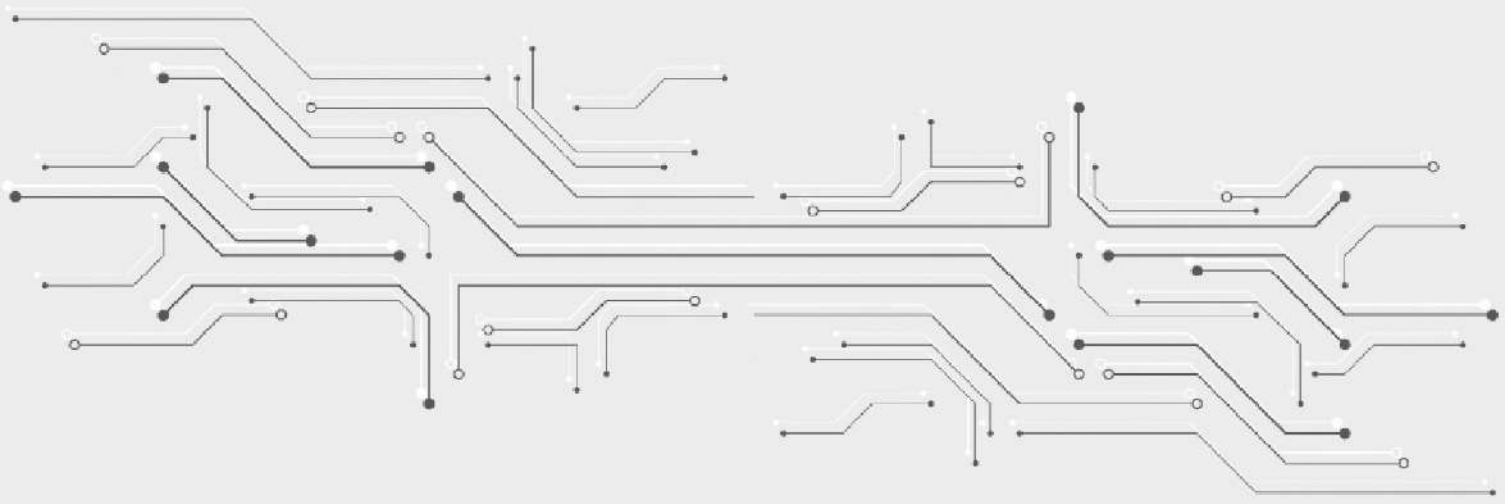
Descargar ahora

C|EH®Certificación Práctica

El C|EH Práctico es un examen 100 % práctico de 6 horas que se entrega en nuestro rango cibernéticoy requiere que demuestre habilidades y destrezas en técnicas de piratería ética como:

- Herramientas de escaneo de puertos (p. ej., Nmap, Hping)
- Detección de vulnerabilidades
- Ataques a un sistema (p. ej., DoS, DDoS, secuestro de sesión, ataques a servidores web y aplicaciones web, inyección SQL, amenazas inalámbricas)
- Metodología de inyección SQL y técnicas de evasión
- Herramientas de seguridad de aplicaciones web (p. ej., Acunetix WVS)
- Herramientas de detección de inyección SQL (p. ej., IBM Security AppScan)
- Protocolos de comunicación

Este es el siguiente paso para convertirse en C|EH®Máster después de haber conseguido tu C|EH® Certificación. Dentro de la C|EH®Práctico, tiene tiempo limitado para completar 20 desafíos para probar sus habilidades y competencia en un rango cibernético basado en el rendimiento. Este examen NO es una simulación e incorpora una red corporativa en vivo de máquinas virtuales y aplicaciones con soluciones para descubrir vulnerabilidades.



C|EH®Maestro

Al completar el C|EH®(Máster), compuesto por el C|EH®y C|EH®(práctico), el C|EH®(Maestro) se otorgala designación. C|EH®Los maestros han demostrado competencia a nivel de maestría en el conocimiento, las habilidades y las capacidades de la piratería ética con un total de 6 horas de prueba para demostrar su competencia. Los 10 mejores en ambos C|EH®y C|EH®Los exámenes prácticos se presentan en el C|EH®Master Global Ethical Hacking Leader Board.

El C|EH®Examen de un vistazo

Detalles del examen	C|EH®(Examen MCQ)	C|EH®(Práctico)
Número de preguntas/desafíosprácticos	125	20
Duración del exámen	4 horas	6 horas
Formato de prueba	Preguntas de respuestas múltiples	Gama cibernética iLabs
Entrega de prueba	EXAMEN ECC, VUE	-
Disponibilidad	-	Aspen-iLabs
Prefijo de examen	312-50 (EXAMEN ECC), 312-50 (VUE)	-
Puntaje de aprobación	Referirse a https://cert.eccouncil.org/faq.html	70%

El C|EH®El programa v12 lo ayuda a desarrollar experiencia en el mundo real en piratería ética a través de C|EH práctico®entorno de práctica. El C|EH®Engage lo equipa con las habilidades para demostrarque tiene lo que se necesita para ser un gran hacker ético.

Nuevo en C|EH®v12, los estudiantes se embarcarán en su primer compromiso de piratería ética emulado. Estecompromiso de 4 fases requiere que los estudiantes piensen críticamente y prueben el conocimiento y las habilidades adquiridas al capturar una serie de banderas en cada fase, demostrando la aplicación en vivo de habilidades y destrezas en un entorno libre de consecuencias a través del nuevo Cyber Range de EC-Council.

A medida que completa su capacitación y laboratorios prácticos, el C|EH®Engage le permite aplicar todo lo que ha aprendido en un simulacro de compromiso de piratería ética. Este compromiso de seguridad de 4 partes le brinda una experiencia real de compromiso de piratería ética de principio a fin contra una organización emulada. Usando nuestro rango de estilo de capturar la bandera, completará su compromiso respondiendo preguntas de "bandera"a medida que avanza.

Tu misión

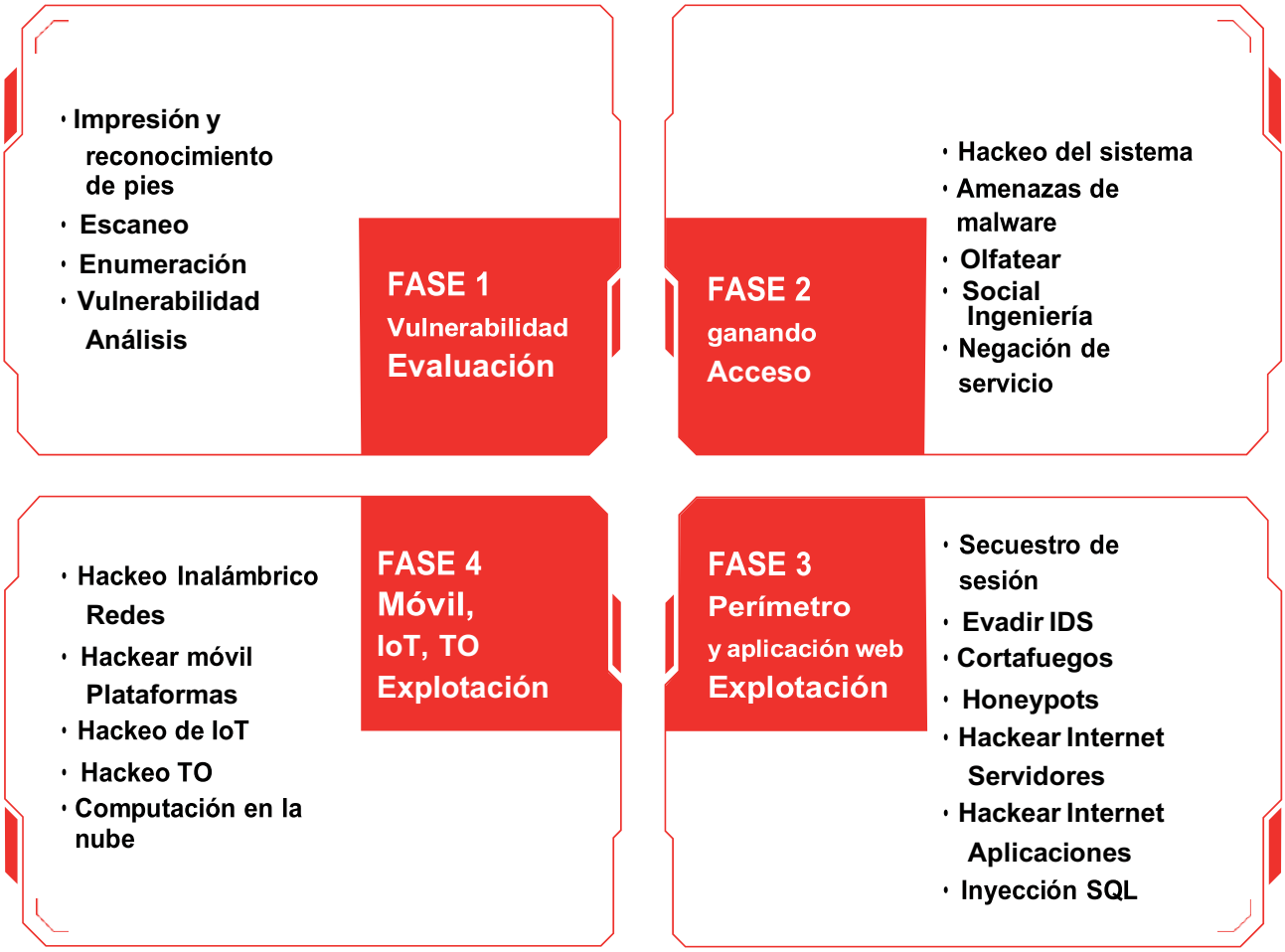
Ya sea que este sea su primer compromiso o esté perfeccionando sus habilidades, ¡prepárese para probar su conocimiento de piratería ética como nunca antes! Una vez que haya practicado a través de los laboratorios guiadosprácticos, es hora de aplicar su conocimiento, asumir la personalidad de hacker y encontrar las vulnerabilidades y debilidades en ABCDorg, todo integrado en nuestro C|EH.®Participar (rango de práctica).

Características de la organización objetivo

ABCD es un TI/ITES a nivel nacional organización	Realista segmentario redes	DMZ y privado las subredes se extienden a lo largo la infraestructura para apoyar varios Unidades de negocios	Varias aplicaciones servidores y soporte de servicios ABCDORG Operaciones
redes reales, operación real sistemas y reales aplicaciones	Privado, acceso dedicado - no compartido recursos	Completamente automatizado despliegue de red con el Consejo de la CE Rango Cibernético	24x7 basado en navegador acceso

Objetivos:

Armado con su plataforma de ataque, Parrot OS y una plétora de herramientas utilizadas por Ethical Hackers, se embarcará en un compromiso de 4 partes para evaluar la postura de seguridad de ABCDorg. Siga el proceso, practique su TTP y experimente lo real en un entorno controlado sin consecuencias, ¡solo la mejor experiencia de aprendizaje para respaldar su carrera como hacker ético!Cada fase se basa en la última a medida que avanza en el compromiso de su ABCDorg.



Pon a prueba tus habilidades y conocimientos con el C|EH®Maestro

Una vez que haya obtenido la certificación y completado su compromiso de piratería ética, estarálisto para desafiar el C|EH supervisado®evaluación práctica y convertirse en un C|EH®
¡Maestro!

Sin una competencia cibernética estimulante, no puede haber progreso. Los competidores lo impulsan a ser lo mejor que puede ser.

El C|EH®Los Desafíos Globales ocurren todos los meses, brindando competencias estilo capturar la bandera que brindan a los estudiantes exposición a varias tecnologías y plataformas nuevas, desde aplicaciones web, OT, IoT, SCADA y sistemas ICS hasta entornos híbridos y en la nube. Nuestra estructura de competencia permite que los hackers éticos luchen por llegar a la cima de la tabla de clasificación cada mes en estos CTF seleccionados de 4 horas. Las banderas basadas en objetivos están diseñadas en torno al proceso de piratería ética, manteniendo lashabilidades actualizadas, probando las habilidades de pensamiento crítico y cubriendo las últimas vulnerabilidades y exploits a medida que se descubren. Alojado 100% en línea en el rango cibernético de EC- Council, los candidatos compiten contra el reloj en compromisos basados en escenarios contra entornos de aplicaciones y redes completamente desarrollados con sistemas operativos reales, redes reales, herramientas y vulnerabilidades para practicar, participar, competir, construir,

El totalmente nuevo C|EH®Desafíos globales

Cada mes se presentará un tema y desafío diferente con competencias estilo Capture-The-Flag que se enfocan enlas destrezas y habilidades básicas de los hackers éticos. Obtenga exposición a nuevas herramientas, concéntreseen nuevos vectores de ataque e intente explotar las vulnerabilidades emergentes mientras obtiene créditos de educación continua y mantiene sus habilidades y certificaciones actualizadas.

¡Nuevos desafíos cada mes!

Mes	Desafío de habilidad
octubre 2022	Los 10 principales vectores de amenazas de aplicaciones web de OWASP
noviembre 2022	Análisis de ransomware/malware
diciembre 2022	Software obsoleto/sin parches
enero 2023	Hackeo del sistema y escalada de privilegios
febrero 2023	Hackeo de aplicaciones web y pruebas de penetración
marzo 2023	Ataque en la nube/Hackeo
abril 2023	Ataques de ingeniería social/phishing
mayo 2023	Ataque/hackeo de IoT
junio 2023	Ataque/hackeo de red Wi-Fi
julio 2023	Ataque DOS/DDoS
agosto 2023	Ataque Móvil/Hackeo
septiembre 2023	Ataques cibernéticos a la cadena de suministro

Competir hasta todos te conocen

Como Ethical Hacker, lucharás para llegar a la cima de las tablas de clasificación mensuales mientras corres contrarreloj en estos desafíos CTF de 4 horas. Abierto todo el mes, la elección es tuya en cuanto a cuándo competir, ¡pero preséntate listo! Todo lo que necesita es una conexión, competir a través de su navegador, proporcionamos la plataforma de ataque, los objetivosy todas las herramientas, ¡usted trae las habilidades para ganar!

Requisitos previos

Todo lo que necesitas es una conexión, y puedes competir a través de tu navegador. Proporcionamos la plataforma de ataque, los objetivos y todas las herramientas necesarias.

¡Tú traes las habilidades para ganar!

Ejemplo de competencia

Vista previa de los próximos desafíos

Tema:
Secuestro de datos/
Análisis de malware

Breve: Ha sido llamado por una reputada MNC atacada con malware recientemente. Esto bloqueó sus servicios y logró infectar a una gran cantidad de clientes que también estaban usando su solución. El equipo de respuesta a incidentes logró extraer parte del código, y ahora su trabajo consiste en aplicar ingeniería inversa al malware e identificar los algoritmosde cifrado utilizados, así como identificar cualquier rastro de servidores de comando y control que puedan ser útiles para las fuerzas del orden.

Tema:
Solicitud
Endurecimiento

Breve: Su empleador, una gran institución financiera, sufrió una brecha en la que los piratas informáticos pudieron inyectar código en una aplicación webque expuso datos confidenciales de los clientes. Su empresa se ha enfrentado a un tremendo escrutinio por parte del público y ha tenido que pagar multas a sus reguladores. Ha realizado una serie de pruebas manuales y automatizadas contra la aplicación web para identificar debilidades y proporcionar contramedidas recomendadas al equipo de seguridad de la aplicación.

Características:

1. Nueva Metodología de Aprendizaje: Aprender – Certificar – Participar – Competir
2. Compite: ¡nuevos desafíos cada mes para poner a prueba tus habilidades para el trabajo!
3. Cumplimiento del 100 % con el marco NICE 2.0
4. Basado en un análisis integral de tareas laborales de toda la industria
5. Laboratorios de aprendizaje práctico
6. Campo de práctica
7. Competiciones comunitarias globales C|EH
8. Hoja de referencia
9. Cobertura del último malware
10. Programa intensivo de laboratorio (cada objetivo de aprendizaje se demuestra mediante laboratorios)
11. Programa práctico (más del 50 % del tiempo de capacitación se dedica a los laboratorios)
12. El entorno de laboratorio simula un entorno en tiempo real (la configuración de laboratorio simula redes y plataformas de la vida real)
13. Cubre las últimas herramientas de piratería (basado en Windows, macOS y Linux)
14. El último sistema operativo cubierto y un entorno de prueba parcheado
15. Todas las capturas de pantalla de la herramienta se reemplazan con la última versión
16. Todas las diapositivas de la lista de herramientas se actualizan con las herramientas más recientes
17. Todas las diapositivas de contramedidas están actualizadas.

Actualizaciones tecnológicas:

1. Marco MITRE ATTACK
2. Modelo de diamante de análisis de intrusión
3. Técnicas para establecer la persistencia
4. Evadir NAC y seguridad de punto final
5. Computación en la niebla
6. Computación perimetral
7. Computación en red

Sistema operativo actualizado

ventanas 11	**Servidor Windows 2022**
Seguridad de loros	**Servidor Windows 2019**
Androide	**Ubuntu linux**

Contenido del curso

3000+ Páginas del manual del estudiante	**1900+** Páginas del manual de laboratorio
3500+ Herramientas de piratería y seguridad	**220** Prácticas prácticas de laboratorio
519 Técnicas de ataque	**20** Módulos actualizados

Roles de trabajo comunes para C|EH

- Auditor de Seguridad de la Información de Nivel Medio
- Auditor de Ciberseguridad
- Administrador de seguridad
- Administrador de seguridad de TI
- Analista de Ciberdefensa
- Analista de evaluación de vulnerabilidades
- Analista de advertencias
- Analista de Seguridad de la Información 1
- Analista de seguridad L1
- Administrador de seguridad de Infosec
- Analista de ciberseguridad nivel 1, nivel 2 y nivel 3
- Ingeniero de Seguridad de Redes
- Analista de Seguridad SOC
- Analista de seguridad
- Ingeniero de redes
- Consultor sénior de seguridad
- Gerente de Seguridad de la Información
- Analista sénior de SOC
- Arquitecto de soluciones
- Consultor de Ciberseguridad

C|EH®Información del examen v12

C|EH®(ANSI)

Título del examen:
Hacker ético certificado (ANSI)

Código de examen:
312-50 (EXAMEN ECC), 312-50 (VUE)

Numero de preguntas:
125

Duración:
4 horas

Disponibilidad:
ECCEXAM/VUE

Formato de prueba:
Opción multiple

Puntaje de aprobación:Consulte https://cert.eccouncil.org/faq.html

C|EH®PRÁCTICO

Título del examen:
Hacker Ético Certificado (Práctico)Número de desafíos prácticos: 20

Duración:
6 horas

Disponibilidad: iLabs

de ASPEN

Formato de prueba:

Gama cibernética iLabs

Puntaje de

aprobación:

70%

Capacitación	Duración
5 Días	40 Horas

Opciones de entrenamiento

iLearn (autoaprendizaje)

Esta solución es un entorno asíncrono de autoaprendizaje en un video formato de transmisión

iWeek (en vivo en línea)

Esta solución es en vivo, en línea, dirigida por un instructor curso de entrenamiento

Clase maestra

La oportunidad de aprender de instructores de clase mundial y colaborar con Los mejores profesionales de la infoseguridad.

Socio de capacitación (en persona)

Esta solución ofrece capacitación “presencial” paraque pueda obtener el beneficio de colaborar con sus compañeros y adquirir habilidades del mundo real, convenientemente ubicado en su patio trasero.

La NUEVA evaluación de vulnerabilidad y

Pista de prueba de penetración (VAPT)
Cómo lograr C|EH®¡y más allá!

C|ND Certified Network Defender » C|EH Certified Ethical Hacker » C|PENT Certified Penetration Testing Professional

Confiado por

EMPRESAS FORTUNE 500

C|EH®v12
Reconocimiento / Endoso / Mapeo

NICE — *Mapeo 100% al NICE Workforce Framework para la Ciberseguridad*

La Iniciativa Nacional para la Educación en Seguridad Cibernética (NIC)

ANSI ACCREDITED — ANSI Accredited Program PERSONNEL CERTIFICATION 17024

Estándares Nacionales Americanos Instituto (ANSI)

COMMITTEE ON NATIONAL SECURITY SYSTEMS — CNSS

Comité Nacional Sistemas de Seguridad (CNSS)

Estados Unidos Departamento de Defensa (DoD)

nicf NATIONAL INFOCOMM COMPETENCY FRAMEWORK — Jointly developed by IDA and WDA

Infocomunicación Nacional Marco de competencias (NICF)

MSC MALAYSIA Spearheading Transformation

MSC

KOMLEK

Por qué la gente ama a C|EH®

“C|EH®La certificación hizo que mi CV fuera sobresaliente en comparación con mis compañeros. Me ha dado un puesto emocionante en EY”.

Sidhant Gupta,Consultor sénior de seguridad, nominado al Salón de laFama (CE-Consejo, Cómo C|EH®Me ayudó, 2021)

“Qué C|EH®te da es una vista de 360 grados. Entonces, lo que te deja es un deseo de aprendermás y más sobre un tema infinitamente grande donde el individuo importa poco y el equipo importa mucho”.

Lorenzo Neri,Especialista en seguridad, finalista del Salón de la Fama

---

“Convertirse en C|EH®Master me ha dado la creencia de que puedo progresar más en la industriade la ciberseguridad y me inspiró a ir más allá con mis calificaciones profesionales, lo que espero me permita obtener la acreditación CREST”.

Pablo Mahoney,Gerente de seguridad y resiliencia de redes para un gran implementador de cajeros automáticos,finalista del Salón de la Fama de 2021

“Me gusta mucho la formación práctica, los laboratorios son muy intuitivos. El programa lo guía a través de cada paso y lo desglosa para que pueda entenderlo”.

Ricardo Medlín,Analista de Pentester y Ciberseguridad, un infante de marina en servicio activo y miembro recién incorporado de la C|EH®Salón de la fama (EC-Council, An Active Duty Marine's Journey,2021)

Descubra por qué C|EH®cuenta con la confianza de organizaciones de todo el mundo!

Durante 20 años, los programas de seguridad cibernética de EC-Council han empoderado a los profesionales de la seguridad cibernética de todo el mundo para ejercer su capacitación y experiencia para combatir los ataques cibernéticos. El Salón de la Fama celebra a aquellas personas que han sobresalido, logrado y fomentado un espíritu deliderazgo entre sus colegas y compañeros dentro de la comunidad cibernética.

97% **Calificó los temas del programa como directamente relevantes para las amenazas actuales del mundo real.**

63% **Reportó un aumento de sueldo directo o una promoción después de obtener su C|EH®Certificación.**

95% **Respondió siendo capaz de mejorar la seguridad organizacional después de completar el programa.**

Descarga el C|EH®Informe del salón de la fama

Acerca de
EC-Council

El único propósito de EC-Council es construir y perfeccionar la profesión de ciberseguridad a nivel mundial. Ayudamos a individuos, organizaciones, educadores y gobiernos a abordar los problemas de la fuerza laboral global mediante el desarrollo y la selección de programas educativos de seguridad cibernética de clase mundial y sus certificaciones correspondientes. También brindamos servicios de ciberseguridad a algunas de las empresas más grandes del mundo. Con la confianza de 7 de Fortune 10, 47 de Fortune 100, el Departamento de Defensa, la Comunidad de Inteligencia, la OTAN y más de 2000 de las mejores universidades, colegios y empresas de formación, nuestros programas han proliferado en más de 140 países. Han puesto el listón en la educación en ciberseguridad. Mejor conocido por los programas Certified Ethical Hacker, estamos dedicados a equipar a más de2,30,000 soldados de la era de la información con el conocimiento, las habilidades, y habilidades requeridas para luchar y ganar contra los adversarios de sombrero negro. EC-Council desarrolla capacidades cibernéticas individuales y de equipo/organización a través del programa Certified Ethical Hacker, seguido de una variedad de otros programas cibernéticos, que incluyen Usuario certificado de computadora segura, Investigador forense de piratería informática, Analista de seguridad certificado, Defensor de red certificado, Analista SOC certificado, Analista de inteligencia de amenazas certificado, controlador de incidentes certificado y director de seguridad de la información certificado.

Somos una organización acreditada por ANSI 17024 y hemos obtenido el reconocimiento del Departamento de Defensa bajo la Directiva 8140/8570 en el Reino Unido por parte de GCHQ, CREST y varios otros organismos autorizados que influyen en toda la profesión.

Fundado en 2001, EC-Council emplea a más de 400 personas en todo el mundo con diez oficinas globales enEE. UU., Reino Unido, Malasia, Singapur, India e Indonesia. Sus oficinas en EE. UU. están en Albuquerque, NM y Tampa, FL.

Obtenga más información en www.eccouncil.org

EC-Council

Envia un Correo a:
academiaciber@tgk.com.mx

Siguenos en nuestras redes