

C|EH v13

**CONVIÉRTETE EN
UN HACKER ÉTICO
CERTIFICADO**

Impulsado por Capacidades de IA

APRENDE | CERTIFÍCATE | PARTICIPA | COMPITE

EC-Council **C|EH**^{v13}

Certified Ethical Hacker

Construye tu carrera con la certificación de hacking ético **más demandada**

Clasificada en **1º lugar** entre las certificaciones de hacking ético por ZDNet

Clasificada dentro de las **10 principales** certificaciones de ciberseguridad

Clasificada en **4.º lugar** entre las **50 principales** certificaciones líderes en ciberseguridad

01 La **certificación N°1** del mundo por más de 20 años – Hacking Ético

01 **Primeros en la industria:** EC-Council introduce cursos de ciberseguridad

12 CEH se ubica en el puesto 12 entre las **75 certificaciones de TI** mejor pagadas en EE. UU. y a nivel mundial.

97% Indicaron que las habilidades adquiridas en CEH ayudaron a **proteger sus organizaciones.**

95% Elige CEH para el **Crecimiento Profesional**

92% De los gerentes de contratación prefieren candidatos con la certificación CEH para puestos que requieren **habilidades de hacking ético**

45% Los roles de trabajo en ciberseguridad están mapeados a la certificación CEH en 2024, en comparación con más de 20 roles en 2022.

Los roles de trabajo en ciberseguridad están mapeados a la certificación CEH en 2024, en comparación con más de 20 roles en 2022.

1 de cada 2 profesionales recibió ascensos después de completar el CEH

CEH es la única certificación de hacking ético, demandada globalmente, que cubre los dominios centrales de la ciberseguridad y cuenta con reconocimiento y acreditaciones internacionales, además de ofrecer una mayor tasa de empleabilidad.

Asegura el futuro de tu carrera en ciberseguridad con IA

La demanda de profesionales de ciberseguridad con habilidades en IA está en aumento.

Las habilidades en IA ya no son opcionales; son esenciales

42%

de las grandes empresas utilizan activamente IA, y el 59% de los primeros adoptantes planea aumentar la inversión y acelerar la integración de IA (IBM, 2024)

40%

aumento en la demanda de especialistas en Inteligencia Artificial y Aprendizaje Automático (Foro Económico Mundial, 2023)

96%

de los líderes de seguridad consideran que las soluciones de IA son esenciales para contrarrestar amenazas impulsadas por IA debido a su velocidad y efectividad (Darktrace, 2024)

87%

de los líderes empresariales esperan que al menos una cuarta parte de su fuerza laboral necesitará capacitarse en IA (IBM, 2024)

IA en las Amenazas de Ciberseguridad

83%

notan alteraciones tangibles en las metodologías de ataque en medio de la revolución de la IA (EC-Council, 2024)

66%

admiten no estar preparados para los embates cibernéticos impulsados por IA (EC-Council, 2024)

Contramedidas

90%

de los costos por fraude puede reducirse mediante modelos de IA en escenarios específicos donde el análisis de datos de comportamiento se aplica de manera efectiva (IBM, 2024)

AI

y la automatización redujo el impacto de las brechas en un 30%, ahorrando a las empresas USD 850.000 y reduciendo los ciclos de vida de las brechas en 108 días (IBM, 2023)

*McAfee Report. ~Darktrace. †Forbes. *Projected by Future of Jobs Report 2023.
~2023 Emerging Jobs Report, LinkedIn.

Obtén dominio en ciberseguridad para el éxito en el mundo real con **Certified Ethical Hacker v13**

¿Por qué deberías unirte a la revolución de la IA con el programa Certified Ethical Hacker?

Al unirte a la revolución de la IA como Certified Ethical Hacker, adquirirás la experiencia necesaria para navegar en el mundo de última generación de la ciberseguridad.

Los Hackers Éticos Certificados, formados en la última versión CEH v13, están equipados con herramientas y técnicas impulsadas por IA para identificar, explotar y asegurar vulnerabilidades en sistemas y redes. Aprenderás a aprovechar la IA para automatizar la detección de amenazas, predecir brechas de seguridad y responder rápidamente a incidentes cibernéticos. Además, adquirirás las habilidades necesarias para asegurar tecnologías impulsadas por IA frente a posibles amenazas. Esta combinación de hacking ético y capacidades de IA te ubicará a la vanguardia de la ciberseguridad, preparado para defender a organizaciones de diversas industrias contra amenazas avanzadas y adaptarte a desafíos en constante evolución.

Amplifica tu ventaja como Hacker Ético Certificado impulsado por capacidades de IA:

Conocimiento Avanzado: Como Hacker Ético Certificado impulsado por IA, poseerás un conocimiento profundo de las metodologías de hacking ético, mejorado con técnicas avanzadas de IA.

Integración de IA: Integrarás eficazmente la IA en cada fase del hacking ético, desde el reconocimiento y el escaneo hasta la obtención y mantenimiento de acceso, y la cobertura de tus huellas.

Automatización y Eficiencia: Aprovecharás la IA para automatizar tareas, aumentar la eficiencia y detectar amenazas sofisticadas que los métodos tradicionales podrían pasar por alto.

Defensa Proactiva: Con la IA a tu disposición, estarás equipado para la búsqueda proactiva de amenazas, la detección de anomalías y el análisis predictivo, permitiendo prevenir ciberataques antes de que ocurran.

Cómo CEH v13 impulsado por IA redefine tu carrera en ciberseguridad

- | Experimenta el primer programa de hacking ético del mundo impulsado por IA.
- | Domina las cinco fases del hacking ético integradas con IA.
- | Alcanza un 40% de eficiencia y duplica tu productividad con habilidades impulsadas por IA
- | Aprende a hackear sistemas de IA.
- | Conviértete en un experto en IA con laboratorios prácticos para desarrollar habilidades en IA.
- | Domina las últimas técnicas de ataque avanzadas, tendencias y contramedidas.
- | Obtén experiencia práctica con 221 laboratorios, vectores de ataque y herramientas de hacking.
- | Practica con más de 550 técnicas de ataque
- | Explora más de 4.000 herramientas de seguridad y hacking de nivel comercial.
- | Sigue un marco de aprendizaje único de cuatro fases: Learn, Certify, Engage, Compete.
- | Practica hackeando una organización real en un cyber range en vivo.
- | Valida tus habilidades en un examen práctico de 6 horas o en un examen teórico de 4 horas.
- | Compite con hackers en competencias CTF globales sobre los temas más recientes.
- | Obtén la certificación No.1 en hacking ético reconocida a nivel mundial.
- | Accede a una certificación aprobada y acreditada por U.S. DoD 8140, ANAB 17024 y NCSC.
- | Cumple con los exigentes estándares de NICE 2.0 y del marco NIST.
- | Accede a oportunidades laborales en organizaciones líderes, incluidas empresas Fortune 500, entidades gubernamentales y firmas del sector privado.

Qué hay de nuevo en **CEH v13**

El CEH v13 no solo ofrece una amplia cobertura práctica, sino que también integra IA en las cinco fases del hacking ético:



Recibe entrenamiento CEH desde cualquier lugar con nuestros instructores de clase mundial

- 1. En línea en vivo
- 2. Videoclases a tu propio ritmo
- 3. Entrenamiento presencial
- 4. Masterclass

Domina la IA para **automatizar tareas de hacking ético** y para hackear y defenderte de sistemas basados en IA

y aumentar tu **eficiencia** en las tareas **en un 40%** en tu rol laboral.

Desarrolla una mentalidad de hacker: Domina las 5 fases del hacking ético y adquiere habilidades en IA para automatizarlas

1. Reconocimiento

| Aprende a recopilar información esencial sobre tu objetivo

2. Escaneo de Vulnerabilidades

| Adquiere la capacidad de identificar debilidades en el sistema objetivo

3. Obtención de Acceso

| Aprende a explotar activamente las vulnerabilidades identificadas

4. Mantenimiento de Acceso

| Desarrolla habilidades para mantener acceso continuo a los sistemas objetivo

5. Borrado de Huellas

| Domina el arte de eliminar cualquier rastro de tus actividades

Aprende Herramientas AI :

- ShellGPT
- ChatGPT
- FraudGPT
- WormGPT
- DeepExploit
- Nebula
- Veed.io

Y muchas más!

Aprende a hackear sistemas de IA basados en las 10 principales vulnerabilidades y amenazas de ataques de IA según OWASP

En CEH v13, no solo dominarás la ciberseguridad impulsada por IA, sino que también aprenderás a hackear sistemas de IA. Esta formación integral te equipa con habilidades avanzadas impulsadas por IA, mejorando tu capacidad para ejecutar tareas de ciberseguridad con hasta un 40% más de eficiencia, mientras aumenta significativamente tu productividad.

- Inyección de Prompts
- Manejo Inseguro de Salidas
- Envenenamiento de Datos de Entrenamiento
- Denegación de Servicio del Modelo
- Vulnerabilidades en la Cadena de Suministro
- Divulgación de Información Sensible
- Diseño Inseguro de Plugins
- Agencia Excesiva
- Dependencia Excesiva
- Robo de Modelo

CEH v13 Adquiere habilidades para enfrentar IA con IA

Tu campo de entrenamiento definitivo para dominar habilidades de ciberseguridad impulsadas por IA

CEH v13 equipa a los profesionales con habilidades avanzadas para mejorar sus técnicas de hacking y aprovechar la IA. Adquiere la experiencia para:

- Impulsar un 40% de eficiencia en tareas de ciberseguridad
- Duplicar tu productividad con métodos impulsados por IA
- Dominar la aplicación de IA en ciberseguridad
- Aprender a hackear sistemas de IA
- Explorar múltiples herramientas de IA y GPT
- Automatizar tareas repetitivas
- Detectar amenazas avanzadas
- Tomar decisiones informadas utilizando análisis mejorado por IA
- Adaptarte a amenazas en evolución mediante aprendizaje impulsado por IA
- Mejorar los reportes con información potenciada por IA

CEH v13: La primera certificación de hacking ético del mundo con un marco de aprendizaje de 4 fases impulsado por IA

El CEH v13 es un programa de formación especializado y único en su tipo que te ayuda a adquirir experiencia en hacking ético, IA y aprendizaje automático. Con laboratorios prácticos, exámenes teóricos y prácticos, una simulación de compromiso de hacking ético en redes activas y una competencia global de hacking, este programa garantiza que domines las habilidades más demandadas para destacar y sobresalir en la industria de la ciberseguridad.

Este marco de aprendizaje no solo ofrece un programa de formación integral para prepararte para el examen de certificación, sino también la experiencia de laboratorio práctico y entorno de práctica más sólida y profunda de la industria.

Domina habilidades de hacking ético y de IA que van más allá de la certificación

Aprender

Material del curso
Cyber Range
Adquirir habilidades

1

Certificar

Examen práctico basado en
conocimientos
Obtener reconocimiento

2

Compromiso

Cyber Range en vivo
Ganar experiencia

3

Competir

Competencia Global de
Hacking Ético
Ganar respeto

4

¡Vence a los hackers en su propio juego con CEH v13! Una forma revolucionaria de aprender hacking ético

1. Aprende

20 módulos

Más de 2.500 páginas de manual del estudiante

2.000 páginas de manual de laboratorio

Más de 221 laboratorios prácticos para entrenar vectores de ataque y herramientas de hacking

Habilidades con IA integradas en las 5 fases del marco de hacking ético

Hacking de sistemas de IA basado en las 10 principales vulnerabilidades de OWASP

Más de 4.000 herramientas de hacking y seguridad

Aprende a hackear múltiples sistemas operativos (Windows 11, servidores Windows, Linux, Ubuntu, Android)

Más del 50% del tiempo de formación está dedicado a laboratorios

2. Certificar

Examen Basado en Conocimientos
(ANAB ISO 17024 y US DoD 8140)

4 horas

125 preguntas de opción múltiple

Examen Practico
(ANAB ISO 17024 and US DoD 8140)

6 horas

20 preguntas basadas en escenarios reales

3. Compromiso

4000 herramientas de hacking

550 técnicas de ataque

Realiza una asignación de hacking ético del mundo real

Aplica las 5 fases

1. Reconocimiento	4. Mantenión de acceso
2. Escaneo	5. Cubrir tus huellas
3. Obtención de acceso	

4. Competencia

Nuevos desafíos cada mes

Competencia CTF de 4 horas

Compite con tus pares en todo el mundo

Hackea tu camino hasta lo más alto del ranking

Enfócate en nuevos vectores de ataque

Explota vulnerabilidades emergentes

Los desafíos incluyen:

- | | |
|--------------------------------------|--|
| ○ Ransomware | ○ • Hacking y pruebas de penetración en aplicaciones web |
| ○ Endurecimiento de aplicaciones web | ○ • Ingeniería inversa |
| ○ Software sin parches | ○ • Criptografía |
| ○ Hacking de sistemas | ○ • Encriptación |
| ○ Explotación de servicios | ○ • Hacking de redes en la nube |
| ○ Respuesta a incidentes | ○ • ICS/SCADA |
| ○ Análisis forense | |

Aprende

Aprende hacking ético con el revolucionario CEH v13 — un cambio total para quienes aspiran a convertirse en hackers éticos.

Con 20 módulos de vanguardia, adquirirás las habilidades esenciales necesarias para dominar el panorama de la ciberseguridad. CEH no solo sigue el ritmo: lidera la evolución, adaptándose a los sistemas operativos, exploits, herramientas y técnicas de hacking más recientes para asegurarte de que siempre estés un paso adelante.

Sumérgete en el futuro de la ciberseguridad con una formación que integra IA en las cinco fases del hacking ético, desde el reconocimiento y el escaneo hasta la obtención de acceso, el mantenimiento del acceso y el borrado de huellas. Aprovecharás el poder de la IA para potenciar tus técnicas de hacking y alterar sistemas de IA, logrando una eficiencia 10 veces mayor en tu rol de ciberseguridad.

CEH v13 no es solo una certificación; es una experiencia completamente inmersiva. CEH combina formación integral basada en conocimiento con laboratorios prácticos inmersivos para asegurar una experiencia de aprendizaje equilibrada. Trabajarás con objetivos reales, herramientas y sistemas vulnerables en un entorno controlado, desarrollando habilidades reales que te permitirán aplicar tu experiencia con confianza en cualquier escenario.

¡Prepárate para transformar la forma en que hackeas y proteges el mundo digital!

Temario del Curso

Obtén la ventaja de la IA con 20 módulos potentes del CEH v13



Aprender	Temario del Curso
Module 01 Introducción al Hacking Ético	Aprende los fundamentos y los temas clave en seguridad de la información, incluyendo los conceptos básicos del hacking ético, los controles de seguridad de la información, las leyes relevantes y los procedimientos estándar.
Module 02 Footprinting y Reconocimiento	Aprende a utilizar las técnicas y herramientas más recientes para footprinting y reconocimiento, una fase crítica previa al ataque dentro del hacking ético.
Module 03 Escaneo de Redes	Aprende distintas técnicas de escaneo de redes y sus contramedidas.
Module 04 Enumeracion	Aprende diversas técnicas de enumeración, incluyendo exploits de Border Gateway Protocol (BGP) y Network File Sharing (NFS), junto con sus contramedidas asociadas.
Module 05 Análisis de Vulnerabilidad	Aprende a identificar fallas de seguridad en la red, la infraestructura de comunicaciones y los sistemas finales de una organización objetivo. También se incluyen diferentes tipos de evaluación de vulnerabilidades y herramientas de evaluación de vulnerabilidades.
Module 06 Hacking de Sistemas	Aprende sobre las diversas metodologías de hacking de sistemas utilizadas para descubrir vulnerabilidades en sistemas y redes, incluyendo esteganografía, ataques de esteganálisis y cómo cubrir huellas.
Module 07 Amenazas de Malware	Aprende sobre los diferentes tipos de malware (trojanos, virus, gusanos, etc.), APT y malware sin archivos, los procedimientos de análisis de malware y las contramedidas contra malware.
Module 08 Sniffing	Aprende sobre las técnicas de packet sniffing y sus usos para descubrir vulnerabilidades en la red, además de las contramedidas para defenderse contra ataques de sniffing.
Module 09 Ingeniería Social	Aprende los conceptos y técnicas de ingeniería social, incluyendo cómo identificar intentos de robo de información, auditar vulnerabilidades a nivel humano y proponer contramedidas de ingeniería social.
Module 10 Denegación de Servicio	Aprende sobre las diferentes técnicas de ataques de Denegación de Servicio (DoS) y Denegación de Servicio Distribuida (DDoS), además de las herramientas utilizadas para auditar un objetivo y diseñar contramedidas y protecciones contra DoS y DDoS.



Aprender	Temario del Curso
Module 11 Secuestro de Sesión	Aprende las diversas técnicas de secuestro de sesión utilizadas para descubrir debilidades en la gestión de sesiones a nivel de red, autenticación, autorización y criptografía, junto con sus contramedidas asociadas.
Module 12 Evasión de IDS, Firewalls y Honeypots	Aprende sobre firewalls, sistemas de detección de intrusiones (IDS) y técnicas de evasión de honeypots; las herramientas utilizadas para auditar el perímetro de una red en busca de debilidades; y las contramedidas.
Module 13 Hacking de Servidores Web	Aprende sobre los ataques a servidores web, incluyendo una metodología de ataque integral utilizada para auditar vulnerabilidades en infraestructuras de servidores web y sus contramedidas.
Module 14 Hacking de Aplicaciones Web	Aprende sobre los ataques a aplicaciones web, incluyendo una metodología de hacking integral para auditar vulnerabilidades en aplicaciones web y las contramedidas correspondientes.
Module 15 Inyección SQL	Aprende sobre las técnicas de ataque de inyección SQL, técnicas de evasión y las contramedidas contra inyección SQL.
Module 16 Hacking de Redes Inalámbricas	Aprende sobre los diferentes tipos de encriptación, amenazas, metodologías de hacking, herramientas de hacking, herramientas de seguridad y contramedidas para redes inalámbricas.
Module 17 Hacking de Plataformas Móviles	Aprende los vectores de ataque en plataformas móviles, hacking en Android y iOS, gestión de dispositivos móviles, directrices de seguridad móvil y herramientas de seguridad.
Module 18 Hacking de IoT	Aprende los diferentes tipos de ataques a Internet de las Cosas (IoT) y tecnología operacional (OT), metodologías de hacking, herramientas de hacking y contramedidas.
Module 19 Computación en la Nube	Aprende diferentes conceptos de computación en la nube, como tecnologías de contenedores y computación sin servidor, diversas amenazas y ataques en la nube, metodologías de hacking y técnicas y herramientas de seguridad en la nube.
Module 20 Criptografía	Aprende sobre algoritmos de encriptación, herramientas de criptografía, Infraestructura de Clave Pública (PKI), encriptación de correo electrónico, encriptación de discos, ataques de criptografía y herramientas de criptoanálisis.

Laboratorios de Aprendizaje Práctico

Con 221 laboratorios prácticos en nuestro avanzado cyber range, practicarás cada habilidad en máquinas activas y vulnerabilidades del mundo real. Armado con más de 4.000 potentes herramientas de hacking y una variedad de sistemas operativos, obtendrás una experiencia práctica inigualable con las herramientas de seguridad más utilizadas, las vulnerabilidades actuales y los sistemas operativos estándar de la industria.

Este entorno revolucionario pone a tu alcance las principales herramientas de seguridad de la industria y las vulnerabilidades más recientes, todo en una plataforma accesible desde la web. No importa dónde te encuentres, puedes sumergirte en una experiencia del mundo real y salir convertido en una fuerza a tener en cuenta en el ámbito de la ciberseguridad.

Los créditos de la API de OpenAI no están incluidos como parte del programa.

Entorno de Laboratorio

Cyber Range Basado en la Nube

Qué está incluido

Virtualización 100% para una experiencia de aprendizaje completa

Acceso completo a objetivos, redes y herramientas de ataque preconfigurados necesarios para explotarlos:

Sitios web vulnerables preconfigurados

Sistemas operativos vulnerables y sin parches

Entornos completamente interconectados

¡Más de 4.000 herramientas de hacking y mucho más!

Amplia variedad de plataformas objetivo para perfeccionar tus habilidades

550 técnicas de ataque cubiertas

Flags orientadas a objetivos para pensamiento crítico y evaluación de conocimiento aplicado

Cyber range basado en la nube

Certificar

**Demuestra tus habilidades
y capacidades con
exámenes prácticos en
línea**

**Exámenes CEH: Examen
de conocimientos de 4
horas y examen práctico
de 6 horas.**

El Certified Ethical Hacker (CEH) es reconocido globalmente como el estándar de oro para evaluar habilidades de hacking ético. Con CEH v13, tienes la opción de rendir dos exámenes: un examen basado en conocimientos y un examen práctico para obtener la certificación CEH Master. Ambos exámenes están aprobados por el U.S. DoD 8140 y acreditados por ANAB ISO/IEC 17024.

Los profesionales de la industria revisan meticulosamente los dominios de certificación para alinearlos con las demandas actuales del sector. Cada examen se somete a una rigurosa evaluación psicométrica, garantizando una valoración justa y precisa de tu experiencia en hacking ético.

Obtener la certificación CEH y aprobar tanto el examen basado en conocimientos como el examen práctico te otorga la prestigiosa certificación CEH Master. Este reconocimiento avanzado demuestra no solo tu comprensión teórica, sino también tu dominio de las habilidades de hacking ético en escenarios reales, probando que estás listo para destacar en cualquier rol de ciberseguridad.

Resumen de la Certificación

Examen de Conocimientos
4 horas
Examen de opción múltiple

Examen de Habilidades
6 horas
20 desafíos prácticos



Examen CEH Basado en Conocimientos

El examen de conocimientos de CEH es un examen de cuatro horas con 125 preguntas de opción múltiple. Evaluará tus habilidades en amenazas de seguridad de la información, vectores de ataque, detección de ataques, prevención de ataques, procedimientos, metodologías y más. ¡Este examen es reconocido mundialmente como el examen original y más confiable de certificación táctica en ciberseguridad.

Accede a nuestro Esquema del Examen para CEH ([Download Now](#))

Examen Práctico de CEH

El examen práctico de CEH es el primer examen práctico de hacking ético en el mundo en contar con la aprobación de ANAB y del US DoD. El CEH Practical es un examen de 6 horas, 100% práctico, impartido en nuestro Cyber Range, que requiere que demuestres las habilidades y capacidades de las técnicas de hacking ético, tales como:

Herramientas de escaneo de puertos (por ejemplo, Nmap, Hping)

Detección de vulnerabilidades

Ataques a un sistema (por ejemplo: DoS, DDoS, secuestro de sesión, ataques a servidores web y aplicaciones web, inyección SQL y amenazas inalámbricas)

Metodología de inyección SQL y técnicas de evasión

Herramientas de seguridad para aplicaciones web (por ejemplo, Acunetix WVS)

Herramientas de detección de inyección SQL (por ejemplo, IBM Security AppScan)

Protocolos de comunicación

En el CEH Practical, tienes un tiempo limitado para completar 20 desafíos que ponen a prueba tu competencia en un cyber range basado en desempeño.

Este examen NO es una simulación e incorpora una red corporativa en vivo compuesta por máquinas virtuales y aplicaciones con vulnerabilidades reales por descubrir.

CEH Master

Al completar con éxito tanto el Examen de Conocimientos de CEH como el Examen Práctico de CEH, se otorga la designación CEH (Master). Un CEH (Master) representa un alto nivel de competencia en conocimientos, habilidades y capacidades de hacking ético, con un total de 6 horas de evaluación para demostrar su dominio.

Los 10 mejores participantes tanto del Examen de Conocimientos de CEH como del Examen Práctico de CEH aparecen en el CEH Master Global Ethical Hacking Leader Board.

Resumen de los Exámenes CEH

Detalles del Examen	Examen Conocimientos CEH	Examen Práctico CEH
Número de Preguntas / Desafíos Prácticos	125 Preguntas	20 Desafíos Prácticos
Duración de la Prueba	4 Horas	6 Horas
Formato de la Prueba	MCQ	iLabs Cyber Range
Disponibilidad de la Prueba	ECC Exam, Vue	ASPEN, iLabs
Prefijo del Examen	312-50 (ECC Exam), 312-50 (VUE)	-
Puntaje de Aprobación	60% - 85%	60% - 85%

Compromiso

El programa CEH v13 te sumerge en el hacking ético del mundo real a través del dinámico entorno de práctica de CEH. Con CEH Engage, perfeccionarás tus habilidades y demostrarás que tienes lo necesario para desarrollarte como hacker ético.

Nuevo en CEH v13, los estudiantes iniciarán su primer compromiso de hacking ético emulado. Este compromiso de cuatro fases requiere que los alumnos piensen críticamente y pongan a prueba los conocimientos y habilidades adquiridas capturando una serie de flags en cada fase. Esto demuestra la aplicación en vivo de habilidades y capacidades en un entorno sin consecuencias gracias al nuevo “Cyber Range” de EC-Council.

A medida que completes tu entrenamiento y laboratorios, CEH Engage te permite llevar la teoría a la práctica mediante un compromiso de hacking simulado. Navegarás un compromiso realista de cuatro partes, dirigido a una organización emulada. Utilizando un formato de capture-the-flag, avanzarás respondiendo preguntas críticas de flags, obteniendo experiencia práctica en una operación completa de hacking ético.

Tu Misión:

Tanto si este es tu primer compromiso como si estás perfeccionando tus habilidades, ¡preparate para poner a prueba tus conocimientos de hacking ético como nunca antes! Una vez que hayas practicado en los laboratorios guiados prácticos, es momento de aplicar tu conocimiento, asumir la identidad de un hacker y encontrar las vulnerabilidades y debilidades en la organización ABCD (organización ficticia, pero con redes reales y activas), todo construido dentro de nuestro CEH Engage (entorno de práctica).

Características de la Organización Objetivo

- ABCDorg es una organización nacional de TI/ITES
- Redes segmentadas realistas
- Zonas desmilitarizadas (DMZ) y subredes privadas que se extienden a lo largo de la infraestructura para apoyar diversas unidades de negocio
- • Acceso vía navegador 24/7
- Varios servidores de aplicaciones los servicios apoyan las operaciones de ABCDorg
- Redes reales, sistemas operativos reales y aplicaciones reales
- •Acceso privado y dedicado — sin recursos compartidos
- •Despliegue de red totalmente automatizado con el Cyber Range de EC-Council

Objetivos

Armado con tu plataforma de ataque (Parrot OS) y una gran cantidad de herramientas utilizadas por hackers éticos, emprenderás un compromiso de 4 partes para evaluar la postura de seguridad de ABCDorg. Sigue el proceso, practica tus TTP y experimenta lo real en un entorno controlado sin consecuencias. Es la experiencia de aprendizaje definitiva para respaldar tu carrera como hacker ético.

Cada fase se construye sobre la anterior a medida que avanzas en tu compromiso con ABCDorg.

Fase 1

Evaluación de Vulnerabilidades:

Huella y Reconocimiento
Escaneo
Enumeración
Análisis de Vulnerabilidades

Fase 2

Obtención de acceso:

Hacking de sistemas	Ingeniería Social
Amenazas de malware	Denegación de Servicio
Sniffing	

Fase 4

Explotación en Móviles, IoT y OT

Hacking de Redes Inalámbricas	Hacking de IoT
Hacking de Plataformas Móviles	Hacking de OT
	Computación en la Nube
	Criptografía

Fase 3

Explotación de Perímetro y Aplicaciones Web

Secuestro de Sesión	Hacking de Servidores Web
Evasión de IDS, Firewalls y Honeypots	Hacking de Aplicaciones Web
	Inyección SQL

Competir

El verdadero progreso prospera gracias a la competencia—es lo que te impulsa a alcanzar tu máximo potencial y convertirte en el mejor en el juego.

Los desafíos globales de CEH se realizan mensualmente, ofreciendo competencias al estilo capture the flag que brindan a los estudiantes exposición a diversas tecnologías y plataformas nuevas, desde aplicaciones web, OT, IoT, sistemas SCADA e ICS, hasta entornos en la nube e híbridos.

Competirás contra otros ethical hackers en un evento rápido de cuatro horas mientras asciendes en la tabla de clasificación en CTFs curados y diseñados alrededor del proceso de hacking ético. Cada flag basado en objetivos agudiza tus habilidades actuales, pone a prueba tu pensamiento crítico y cubre las vulnerabilidades y exploits más recientes. Realizado completamente en línea en el Cyber Range avanzado de EC-Council, estos compromisos basados en escenarios están configurados en entornos de red y aplicaciones completamente desarrollados con sistemas operativos, redes, herramientas y vulnerabilidades reales. Tendrás la oportunidad de practicar, participar, competir, construir y perfeccionar tus técnicas de hacking mientras te enfrentas a nuevas organizaciones objetivo, todo mientras compites contra el reloj para demostrar tu dominio.

Desafíos Globales de CEH

Cada mes presentará un tema y un desafío diferente, con competencias de estilo capture the flag enfocadas en las habilidades y capacidades centrales de los hackers éticos. Obtén exposición a nuevas herramientas, concéntrate en nuevos vectores de ataque e intenta explotar vulnerabilidades emergentes

Pre-Requisitos

Solo necesitas una conexión a Internet y puedes competir desde tu navegador. Nosotros proporcionamos la plataforma de ataque, los objetivos y todas las herramientas necesarias. ¡Tú aportas las habilidades para ganar!

Oportunidad de ganar prestigiosas insignias CEH Compete cada mes



Ejemplos de competencia (Una vista previa de los desafíos)

Tema: Análisis de ransomware/malware

Resumen: Te han llamado a una multinacional (MNC) de buena reputación que fue recientemente atacada con malware. Este malware bloqueó sus servicios e infectó a una gran cantidad de clientes que estaban usando su software. El equipo de respuesta a incidentes logró extraer parte del código. Ahora, tu trabajo es hacer ingeniería inversa al malware e identificar los algoritmos de cifrado utilizados, además de identificar cualquier rastro de servidores de comando y control que pueda ser útil para las agencias de aplicación de la ley.

Tema: Endurecimiento de aplicaciones

Resumen: Tu empleador, una gran institución financiera, ha sufrido una brecha en la que los hackers pudieron inyectar código en una aplicación web, exponiendo datos sensibles de clientes. Tu empresa ha enfrentado un enorme escrutinio público y debe pagar multas a sus reguladores. Tienes que realizar 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.

(Become an AI Powered Certified Ethical Hacker)

Mantente por delante de las amenazas emergentes:

Nuevas áreas de enfoque y tendencias en CEH v13

Formados para pensar fuera de lo común con la mentalidad de un hacker, las personas que cursan el Certified Ethical Hacker (CEH) v13 exploran a fondo los principales ataques OWASP, las brechas en Active Directory, la vulnerabilidad del cifrado tradicional frente a la computación cuántica, la creciente amenaza del ransomware y otros riesgos emergentes, dotando a los estudiantes de estrategias para implementar arquitecturas de confianza cero (zero trust) y otras medidas de ciberseguridad. CEH v13 es completo con el conocimiento más reciente, proporcionando a los profesionales de ciberseguridad las habilidades, herramientas, técnicas y estrategias para defenderse de amenazas cibernéticas modernas, complejas y en tendencia de manera eficaz y eficiente.

Ataques a Active Directory

Ataques de ransomware y mitigación

IA y aprendizaje automático en ciberseguridad

Vulnerabilidades en infraestructura crítica

Detección y respuesta extendidas (XDR)

Riesgos y ataques de la computación cuántica

Criptografía poscuántica

Amenazas de deepfake

Arquitectura de confianza cero

Seguridad en la nube

Desafíos de seguridad en IoT

Vulnerabilidades en infraestructura crítica

Obtén 10 videos de hacking ético en CEH v13 Elite

1. Inteligencia de código abierto (Open Source Intelligence)
2. Wireshark para hackers éticos
3. Hacking ético con Nmap
4. Conceptos esenciales de pruebas de penetración en Windows
5. Secuestro de sesión y técnicas de prevención
6. El poder de los firewalls de próxima generación
7. Fundamentos de seguridad OWASP Top 10
8. Burp Suite: Pruebas de penetración en aplicaciones web
9. Análisis profundo de evaluaciones de red
10. Aplicación práctica de ciudad inteligente segura

Habilidades de CEH mapeadas a 49 roles de trabajo en ciberseguridad

1. Auditor de seguridad de la información de nivel medio.
2. Auditor de ciberseguridad
3. Administrador de seguridad
4. Administrador de seguridad de TI
5. Analista de seguridad de la información 1
6. Administrador de seguridad Infosec
7. Analista de ciberseguridad (Nivel 1, Nivel 2 y Nivel 3)
8. Ingeniero de seguridad de redes
9. Analista de seguridad SOC
10. Ingeniero de redes
11. Consultor senior de seguridad
12. Gerente de seguridad de la información
13. Analista senior de SOC
14. Arquitecto de soluciones
15. Consultor de ciberseguridad
16. Analista de defensa cibernética
17. Analista de evaluación de vulnerabilidades
18. Analista de alertas
19. Analista de fuentes múltiples
20. Respondedor a incidentes de defensa cibernética
21. Especialista en investigación y desarrollo
22. Analista senior de seguridad en la nube
23. Gestión de riesgos de terceros.
24. Caza de amenazas
25. Pentester / Evaluador de penetración
26. Gerente de entrega cibernética (Cyber Delivery Manager)
27. Riesgo de seguridad de aplicaciones
28. Especialista en modelado de amenazas
29. Pruebas de penetración en aplicaciones web
30. Gestión de vulnerabilidades SAP
31. Asesor de entrega de soluciones (Solution Delivery Advisor)
32. Hacker ético
33. Respondedor de amenazas SIEM
34. Ingeniero / Gerente de seguridad de productos
35. Ingeniero de seguridad de endpoints
36. Instructor de ciberseguridad
37. Especialista de Red Team
38. Oficial de protección de datos y privacidad
39. Ingeniero SOAR
40. Ingeniero de seguridad de IA
41. Ingeniero senior de IAM
42. Asesor de seguridad PCI
43. Analista de explotación (Exploitation Analyst – EA)
44. Ingeniero / Analista de soluciones Zero Trust
45. Ingeniero criptográfico
46. Ingeniero de seguridad de IA/ML
47. Especialista en seguridad de machine learning
48. Pentester de IA
49. Consultor de seguridad de IA/ML
50. Consultor de seguridad criptográfica

Información de capacitación CEH v13

Capacitación: 5 días

Duración: 40 horas

Opciones de capacitación

iLearn (Autoestudio)

Esta solución es un entorno asincrónico de autoestudio en un formato de transmisión de video.

iWeek (En línea en vivo)

Esta solución es un curso de capacitación en línea, en vivo, dirigido por un instructor.

Master Class

Esta solución ofrece la oportunidad de aprender de instructores de clase mundial y colaborar con los principales profesionales de seguridad de la información.

Training Partner (Presencial)

Esta solución ofrece capacitación presencial para que puedas beneficiarte de la colaboración con tus compañeros.

CEH empleado por **gobiernos** y las principales empresas **Fortune 500** en todo el mundo

¿Por qué los principales profesionales de la ciberseguridad aman CEH?

"Skills from the CEH program have evolved and are valuable."



Mauricio Fernandes
Systems Architect,
Cisco, USA

"Knowledge I gained from CEH gave me the confidence I needed to step into a role as a security engineer and penetration tester."



Roy Davis
Security Engineer,
Zoom, USA

"Helping organization investigating SolarWinds hack, wouldn't have been possible without CEH."



Giulio Astori
Cyber Security Architect,
Microsoft, USA

"CEH was my first confidence booster and helped land me a job on a Red Team in the government sector."



Farzan Karimi
IT Security Manager,
Google, USA

"CEH made me an authoritative expert on security discussions with our clients."



Kojo Donkor
Security Architect,
Cisco, USA

"CEH helped me be able to understand exactly what I was doing once I finally landed a role in the cybersecurity field."



Lawan Cancer II
Security Analyst,
Morgan Stanley, USA

"CEH has helped me to work on mobile devices and AppSec – Pen testing and reverse engineering."



John Packiaraj
Security Architect,
Visa, USA

"While other certifications talk the talk, CEH walks the walk and is recognized by the department of defense."



Michael Turner
Chief Security Engineer,
Lockheed Martin, USA

"CEH develops a "think outside the box" approach that you cannot get from other skills."



Felipe Munoz
IT Security Director,
Oracle, USA

Reconocimiento/Endoso/ Mapeo de CEH v13



Descubre por qué las organizaciones de todo el mundo confían en la certificación CEH

Durante 20 años, los programas de ciberseguridad de EC-Council han empoderado a profesionales de la ciberseguridad en todo el mundo para aplicar su formación y experiencia en la lucha contra los ciberataques. El CEH Hall of Fame celebra a aquellas personas que han sobresalido, logrado grandes resultados y fomentado un espíritu de liderazgo entre sus colegas y pares dentro de la comunidad cibernética. Hallazgos clave informados por miles de profesionales de la ciberseguridad del CEH Hall of Fame Report:

Descargar el informe CEH Hall of Fame

Más de 1 de cada 2 profesionales recibió ascensos después de CEH

El 97% afirmó que las habilidades que adquirieron en CEH ayudaron a proteger sus organizaciones

El 97% encontró que los laboratorios de CEH imitan con precisión las amenazas cibernéticas del mundo real

El 95% eligió CEH para el crecimiento de su carrera

El 93% dijo que las habilidades obtenidas en CEH mejoraron la seguridad de su organización

El 92% de los gerentes de contratación prefiere candidatos con CEH para trabajos que requieren habilidades de hacking ético

El 92% informó que CEH aumentó su autoestima

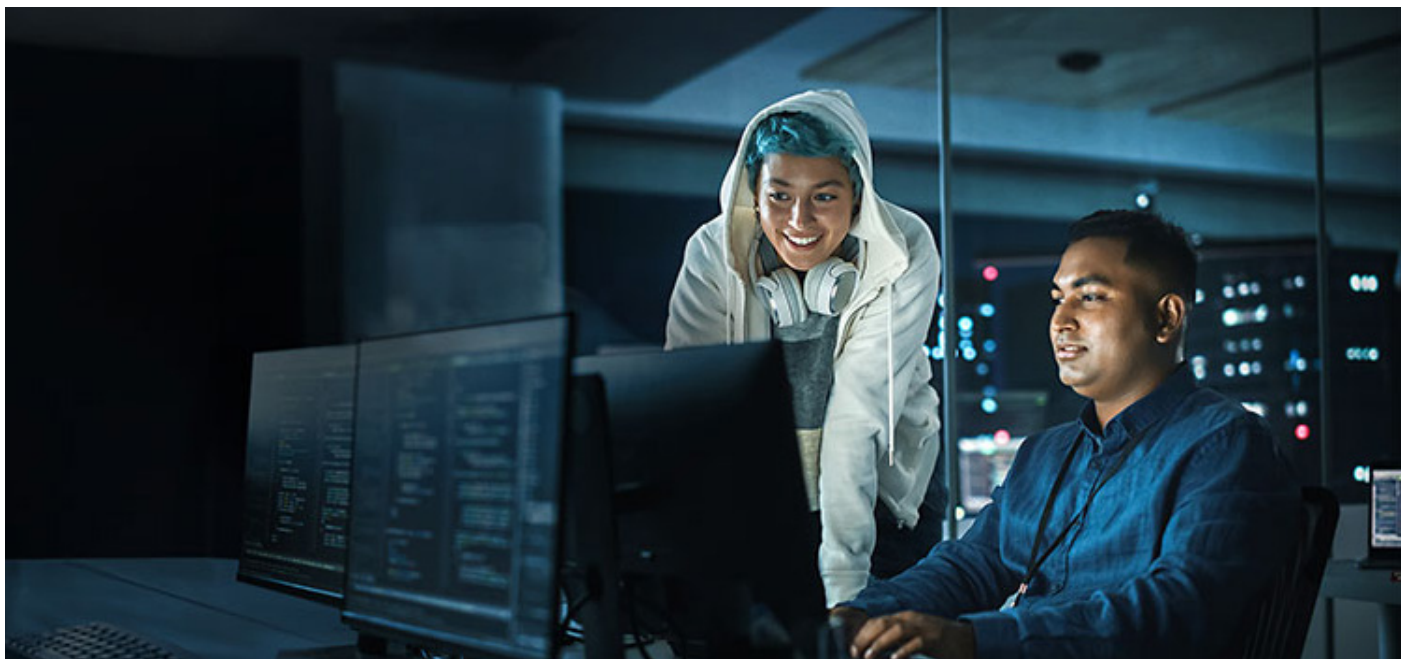
El 88% consideró que CEH es el programa de hacking ético más completo de la industria

El 85% atribuyó a CEH haberlos ayudado a retribuir a la comunidad de ciberseguridad

El 80% inició su carrera en ciberseguridad con CEH

Sobre EC-Council

El único propósito de EC-Council es construir y redefinir la profesión de la ciberseguridad a nivel global.



Ayudamos a individuos, organizaciones, educadores y gobiernos a abordar los problemas globales de fuerza laboral mediante el desarrollo y la selección de programas de educación en ciberseguridad de clase mundial y sus correspondientes certificaciones.

También proporcionamos servicios de ciberseguridad a algunas de las empresas más grandes del mundo. Con la confianza de 7 de las 10 empresas Fortune, 47 de las Fortune 100, el Departamento de Defensa, la comunidad de inteligencia, la OTAN y más de 2.000 de las mejores universidades, colegios e instituciones de formación, nuestros programas han certificado personas en más de 140 países y han establecido el estándar en el campo de la educación en ciberseguridad. Conocidos principalmente por el programa Certified Ethical Hacker (CEH), estamos dedicados a equipar a más de 380.000 “soldados de la era de la información” con los conocimientos, habilidades y capacidades necesarios para luchar y ganar contra los adversarios cibernéticos.

desarrolla capacidades cibernéticas individuales y a nivel organizacional a través de nuestros otros programas también, incluyendo Certified Secure Computer User (CSCU), Computer Hacking Forensic Investigator (CHFI), Certified Security Analyst, Certified Network Defender (CND), Certified SOC Analyst (CSA), Certified Threat Intelligence Analyst (CTIA), Certified Incident Handler (ECIH) y el Certified Chief Information Security Officer (CCISO). Somos una organización acreditada por ANAB bajo ISO/IEC 17024 y hemos obtenido reconocimiento por parte del Departamento de Defensa (DoD) bajo la Directiva 8140/8570, en el Reino Unido por el GCHQ, CREST y varios otros organismos autoritativos. Fundada en 2001, EC-Council emplea a más de 400 personas en todo el mundo, con diez oficinas globales en EE. UU., Reino Unido, Malasia, Singapur, India e Indonesia. Nuestras oficinas en EE. UU. están en Albuquerque, Nuevo México, y Tampa, Florida. Obtén más información en eccouncil.org.



**WE DON'T JUST TEACH
ETHICAL HACKING**

WE BUILD CYBER CAREERS

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

Now Powered by AI

Visit: www.eccouncil.org/ceh