EC-COUNCIL



EC-COUNCIL · PROGRAMA DE HACKING ÉTICO

Certified Ethical Hacker (C|EH AI) v13

Aprenda a atacar como un adversario para encontrar y corregir vulnerabilidades antes de que lo haga un atacante

¿Por qué debería asistir?

CEH v13 forma profesionales capaces de encontrar y corregir vulnerabilidades antes que un atacante. Durante cinco días de formación intensiva, los participantes recorren las cinco fases del hacking ético a lo largo de 20 módulos, con un balance 50/50 entre teoría y práctica en un entorno de laboratorios virtuales.

Esta versión integra la inteligencia artificial en las técnicas ofensivas y defensivas, y amplía la cobertura a la nube, los dispositivos móviles, IoT y OT. Detectar a tiempo una intrusión, un ransomware o una denegación de servicio es la mejor forma de reducir el impacto de un incidente y proteger la continuidad del negocio. Al finalizar la capacitación oficial, usted podrá optar por la credencial C|EH, reconocida a nivel mundial y alineada al 100 % con el marco NICE 2.0.

5 días	20	221	550	50/50
DURACIÓN	MÓDULOS	LABORATORIOS	TÉCNICAS DE ATAQUE	TEORÍA / PRÁCTICA

¿Quién debería participar?

Operaciones de seguridad
Analistas SOC e ingenieros de respuesta a incidentes que necesitan entender cómo piensa y actúa un atacante.

Infraestructura
Administradores de redes y sistemas, e ingenieros y arquitectos de ciberseguridad que protegen la infraestructura.

Pruebas y auditoría
Pentesters, analistas de vulnerabilidades y auditores de seguridad y de TI.

Riesgo y cumplimiento
Responsables de riesgo, cumplimiento y continuidad que deben evaluar la exposición real de la organización.

Objetivos de aprendizaje

- Pensar como un atacante: aplicar el ciclo completo de un ataque, desde el reconocimiento hasta el borrado de huellas, en entornos controlados
- Encontrar y corregir debilidades en redes, sistemas, aplicaciones web, nube, dispositivos móviles, IoT y OT
- Usar la IA en el hacking ético para automatizar fases del ataque y analizar amenazas a sistemas de IA según el OWASP Top 10
- Dominar las herramientas del oficio, con acceso a más de 4.000 herramientas de hacking y seguridad
- Reconocer amenazas actuales: malware, ransomware, ingeniería social, DDoS y ataques a la cadena de suministro
- Prevenir brechas de datos y fortalecer los controles que sostienen la continuidad del negocio
- Validar lo aprendido en un compromiso de 4 fases en el Cyber Range y en competencias mensuales tipo CTF

Las 5 fases del hacking ético

Fase 1 · Reconocimiento | Fase 2 · Escaneo | Fase 3 · Obtener acceso | Fase 4 · Mantener acceso | Fase 5 · Borrar huellas

IA aplicada al hacking ético | Cyber Range y CTF

La IA a lo largo de los 20 módulos
La IA no está en un módulo aparte, sino distribuida en el temario. Algunos ejemplos que coinciden con el brochure que generamos:

- Footprinting: reconocimiento asistido por IA.
- Ingeniería social: deepfakes y phishing generado con IA.
- Malware: análisis apoyado en IA.
- Evasión de IDS y firewalls: técnicas con IA y su detección.
- Aplicaciones web: las vulnerabilidades de IA del OWASP Top 10.

Herramientas de IA que se enseñan
El brochure oficial menciona ShellGPT, ChatGPT, FraudGPT, WormGPT, DeepExploit, Nebula y Veed.io, entre otras. Unas se usan para automatizar tareas del pentester, como ShellGPT, que genera comandos de terminal desde lenguaje natural. Otras se estudian para entender las amenazas: FraudGPT y WormGPT son modelos usados por delincuentes para crear phishing y malware.

Programa del curso

Duración: 5 días

Módulo	Contenido
Módulos 1–4 Día 1	01 **Introducción al hacking ético:** fundamentos, Cyber Kill Chain, MITRE ATT&CK, leyes y estándares. 02 **Footprinting y reconocimiento:** OSINT, DNS, buscadores, redes sociales y reconocimiento con IA. 03 **Escaneo de redes:** descubrimiento de hosts, puertos, servicios y sistemas operativos. 04 **Enumeración:** NetBIOS, SNMP, LDAP, NTP, SMTP, DNS y SMB.
Módulos 5–8 Día 2	05 **Análisis de vulnerabilidades:** clasificación, puntuación CVSS, herramientas e informes. 06 **Hacking de sistemas:** acceso, escalamiento de privilegios, persistencia y borrado de huellas. 07 **Amenazas de malware:** APT, troyanos, ransomware, malware sin archivos y su análisis. 08 **Sniffing:** ARP y DHCP spoofing, envenenamiento DNS y contramedidas.
Módulos 9–12 Día 3	09 **Ingeniería social:** phishing, suplantación de identidad y amenazas internas. 10 **Denegación de servicio:** ataques DoS y DDoS, botnets y estrategias de protección. 11 **Secuestro de sesión:** ataques a nivel de aplicación y de red, y su prevención. 12 **Evasión de IDS, firewalls y honeypots:** técnicas de evasión y detección.
Módulos 13–16 Día 4	13 **Hacking de servidores web:** ataques a servidores, gestión de parches y hardening. 14 **Hacking de aplicaciones web:** OWASP Top 10, APIs y webhooks. 15 **Inyección SQL:** tipos de inyección, evasión de filtros y defensa. 16 **Hacking de redes inalámbricas:** cifrado Wi-Fi, WPA2/WPA3 y Bluetooth.
Módulos 17–20 Día 5	17 **Hacking de plataformas móviles:** Android, iOS y gestión de dispositivos (MDM). 18 **Hacking de IoT y OT:** dispositivos conectados, ICS y SCADA. 19 **Computación en la nube:** contenedores, Kubernetes, serverless y amenazas en la nube. 20 **Criptografía:** algoritmos, PKI, cifrado de correo y discos, y criptoanálisis.

Metodología de cuatro etapas: Aprender, Certificar, Participar, Competir

Aprender: 20 módulos, 221 laboratorios y 550 técnicas de ataque.
Certificar: dos exámenes. El de conocimientos (312-50, 125 preguntas, 4 horas) y el C|EH Práctico: 6 horas, 20 retos sobre máquinas reales.
Participar: un compromiso completo de hacking ético en el Cyber Range, en cuatro fases, de punta a punta como un proyecto real.
Competir: competencias tipo CTF mensuales durante el año, con tabla de posiciones global, para mantener las habilidades al día.

Juntas, las cuatro etapas llevan al alumno de aprender la técnica a demostrarla en un examen práctico, luego a aplicarla en un proyecto completo y finalmente a mantenerla al día compitiendo.

- Entorno: 100 % virtualizado, acceso por navegador las 24 horas, red desplegada automáticamente y acceso privado y dedicado, sin recursos compartidos.
- Resultado: el alumno identifica vulnerabilidades y captura flags en cada fase. Aplica todo lo aprendido en un entorno sin consecuencias reales, como un proyecto profesional.

Examen

Duración: 4 horas

Examen de conocimientos C|EH (ANSI)

Título	EC-Council Certified Ethical Hacker (C|EH) – Versión 13		
Código	312-50	**N.º de preguntas**	125
Formato	Opción múltiple	**Duración**	4 horas
Aprobación	60 % – 85 %, según la forma del examen	**Plataforma**	ECC Exam Portal / Pearson VUE

Examen C|EH Práctico

Retos	20 escenarios reales	**Formato**	Laboratorio en vivo
Duración	6 horas	**Aprobación**	70 %
Plataforma	iLabs Cyber Range		

Requisitos de elegibilidad

- **Con capacitación oficial de EC-Council:** puede presentar el examen sin proceso de elegibilidad.
- **Sin capacitación oficial:** al menos dos años de experiencia en seguridad de la información, solicitud de elegibilidad aprobada y una cuota de US$100.

C|EH Master: valide conocimiento y práctica

Quienes aprueban tanto el examen de conocimientos C|EH (ANSI) como el examen C|EH Práctico obtienen la designación **C|EH Master**, que demuestra que el profesional domina la teoría y además puede ejecutar las técnicas en escenarios reales con tiempo limitado.

Información general

- Material oficial de EC-Council y acceso a los laboratorios iLabs del Cyber Range
- Credencial acreditada por ANAB (ISO/IEC 17024) y reconocida por el DoD 8570/8140
- La certificación es válida por tres años y se renueva con 120 créditos de educación continua (ECE)