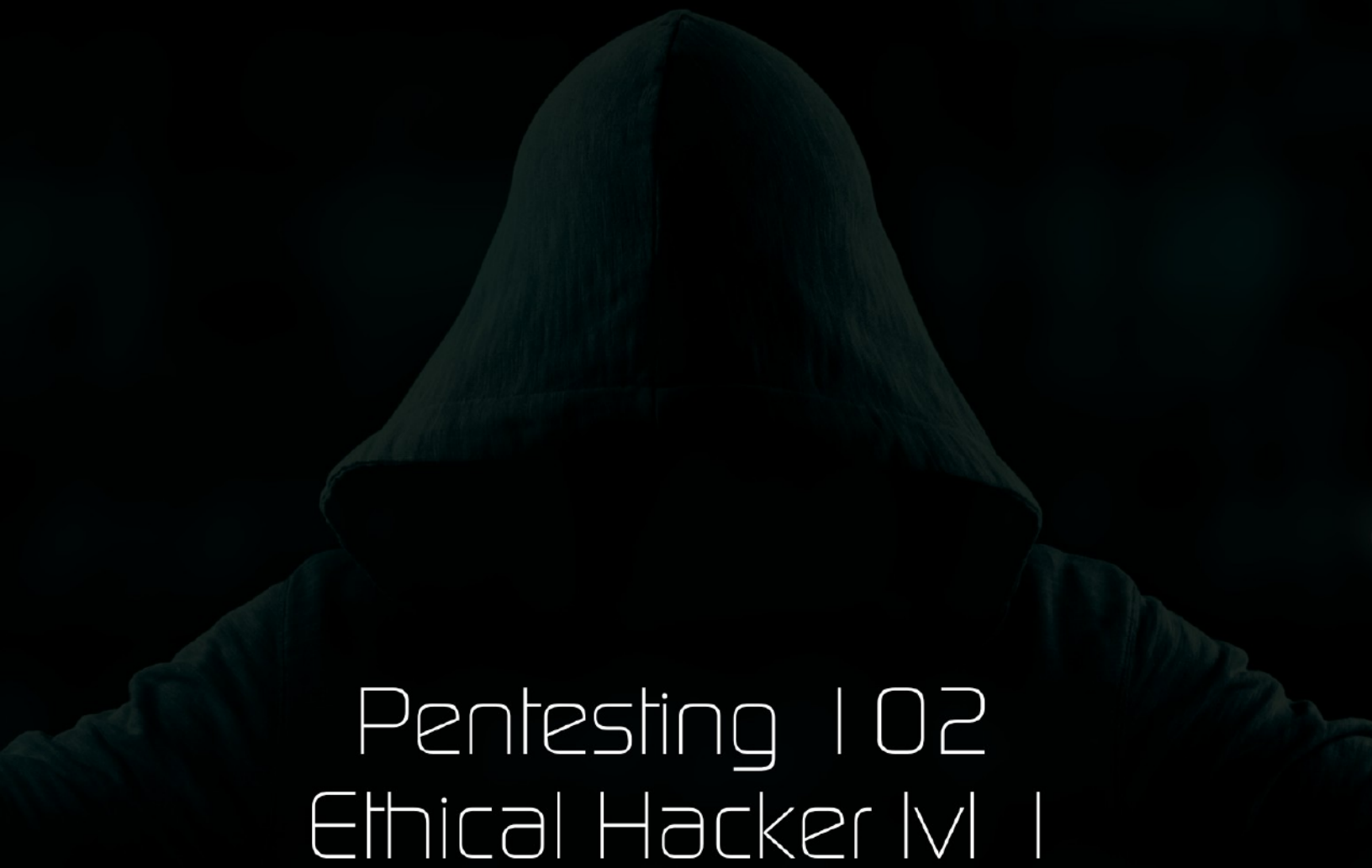
2026



Pentesting 102
Ethical Hacker lvl 1

DESCRIPTIVO DEL CURSO

CSASC

CYBERSECURITY ASSOCIATION COUNCIL

Descripción general

Pentesting 102 - Ethical Hacker Level 1 (Nueva Edición)

Resumen

Pentesting 102 - Ethical Hacker Level 1 es la versión actualizada del curso de entrada (Pentesting 101). Conserva un nivel básico-intermedio, pero fortalece la orientación profesional: método antes que herramienta, OSINT responsable, evidencia mínima, priorización por riesgo y reporte en dos capas (ejecutiva y técnica). El enfoque es formativo y práctico, orientado a comprender cómo y por qué el pentesting aporta valor a la organización.

Público objetivo

- Profesionales de tecnologías de la información.
- Personal de áreas de sistemas, redes o desarrollo.
- Consultores, auditores y responsables de seguridad que inician en ciberseguridad.
- Profesionales que requieren comprender el pentesting como parte del cumplimiento normativo.

Requisitos

No se requiere experiencia previa en hacking, pentesting, normas ISO o marcos NIST. Los conceptos se presentan de manera progresiva y didáctica. Se recomienda familiaridad básica con redes (IP, DNS, HTTP/HTTPS) y sistemas Windows/Linux.

Enfoque metodológico

- Fundamentos teóricos para comprender los conceptos clave.
- Ejemplos prácticos para facilitar la comprensión del contexto real.
- Alineación normativa para relacionar la práctica técnica con estándares y regulaciones.
- Lenguaje accesible sin sacrificar rigor profesional y académico.

Alineación a estándares y marcos

- ISO/IEC 27001:2022 (SGSI) e ISO/IEC 27032:2023 (ciberseguridad).
- NIST Cybersecurity Framework (CSF) 2.0 (gestión del riesgo).
- PCI DSS 4.0 (protección de datos de pago).
- OWASP (aplicaciones web y API) y MITRE ATT&CK (técnicas y tácticas).

Nota: Este curso corresponde a Level 1. El nivel avanzado corresponde a Ethical Hacker Level 2.

Alcance y objetivos

Alcance del curso

- Fundamentos de ciberseguridad y hacking ético.
- Tipos y alcances de las pruebas de intrusión.
- Metodologías y marcos de referencia utilizados en pentesting.
- Introducción al reconocimiento, análisis de vulnerabilidades y explotación controlada.
- Relación del pentesting con la gestión del riesgo y el cumplimiento normativo.
- Importancia del reporte como principal entregable de una prueba de intrusión.
- Sin profundizar en técnicas avanzadas u ofensivas complejas (se abordan en un nivel posterior).

Objetivos de aprendizaje

- Comprender los principios básicos de la ciberseguridad y el hacking ético.
- Identificar qué son las Pruebas de Intrusión y cuál es su propósito dentro de una organización.
- Reconocer los diferentes tipos de pruebas de intrusión y sus alcances.
- Comprender las fases de un proceso de pentesting profesional.
- Interpretar el rol del pentesting dentro de ISO/IEC 27001, ISO/IEC 27032, NIST CSF y PCI DSS 4.0.
- Entender la importancia de la ética, la legalidad y la autorización en las pruebas de seguridad.
- Analizar resultados básicos de pruebas de seguridad y comprender su impacto en el negocio.

Lo que NO es este curso

- Enseña hacking ilegal ni promueve actividades no autorizadas.
- Profundiza en técnicas avanzadas de explotación o ejercicios de Red Team (eso corresponde al nivel avanzado).
- Promueve el uso irresponsable de herramientas ofensivas o prácticas que puedan afectar la operación.

Temario y entregables

Temario (resumen por módulos)

- Módulo 1. Fundamentos de ciberseguridad y hacking ético.
- Módulo 2. Pentesting: conceptos, tipos, alcance y ROE.
- Módulo 3. Ética, legalidad y autorización.
- Módulo 4. Metodologías y marcos (PTES, OSSTMM, OWASP, NIST CSF, PCI DSS, MITRE).
- Módulo 5. Reconocimiento y superficie de ataque (pasivo/activo).
- Módulo 6. Análisis de vulnerabilidades y priorización por riesgo.
- Módulo 7. Validación controlada de hallazgos y evidencia mínima.
- Módulo 8. Post-validación responsable y cierre de la prueba.
- Módulo 9. Reporte profesional (ejecutivo y técnico) y retest.
- Módulo 10. Cierre del curso y ruta de crecimiento.

Entregables

- Plantilla de Alcance y Reglas de Compromiso (ROE).
- Checklists de reconocimiento y validación de hallazgos.
- Guía de priorización por riesgo (impacto, probabilidad y contexto).
- Estructura de reporte ejecutivo y reporte técnico con evidencias y recomendaciones.

Más información e inscripciones: csascouncil.org

Temario detallado

Módulos 1 - 5

Módulo 1. Introducción a la ciberseguridad y al hacking ético

Enfoque: Fundamentos y visión de riesgo.
- CIA, superficie de ataque y gestión de riesgo.
- Hacking ético: propósito, límites y valor para la organización.
- Actividad: activos críticos, amenazas e impactos.

Módulo 2. Pruebas de intrusión (Pentesting)

Enfoque: Propósito, alcance y entregables.
- Tipos de prueba y alcances (caja negra/gris/blanca; interno/externo).
- Pentesting vs. vulnerability assessment y otras evaluaciones.
- Fases generales y entregables (evidencias y reporte).

Módulo 3. Ética, legalidad y autorización

Enfoque: Reglas claras para operar con responsabilidad.
- Autorización formal, límites y confidencialidad.
- ROE: alcance, restricciones y comunicación.
- Stop conditions y manejo de evidencia sensible.

Módulo 4. Metodologías y marcos de referencia

Enfoque: Proceso defendible y alineación normativa.
- PTES/OSSTMM: estructura del proceso de pentesting.
- OWASP (web y API), NIST CSF 2.0, PCI DSS 4.0 y MITRE ATT&CK.;

Módulo 5. Reconocimiento y superficie de ataque

Enfoque: Descubrimiento de activos con OSINT responsable.
- Reconocimiento pasivo/activo y mapeo de exposición.
- Documentación con evidencia mínima suficiente, sin afectar la operación.

Temario detallado

Módulos 6 - 10

Módulo 6. Análisis de vulnerabilidades y priorización

Enfoque: Detectar, validar y priorizar por riesgo.
- Validación y control de falsos positivos/negativos.
- Severidad vs prioridad: impacto, probabilidad y contexto.

Módulo 7. Validación controlada de hallazgos

Enfoque: Demostrar impacto sin comprometer la operación.
- Pruebas controladas y mínima invasión.
- Evidencia mínima aceptable y control de datos.

Módulo 8. Post-validación responsable y cierre

Enfoque: Cierre limpio y buenas prácticas.
- Limpieza responsable y resguardo de evidencias.
- Lecciones aprendidas y oportunidades de mejora.

Módulo 9. Reporte profesional y comunicación

Enfoque: Reporte en dos capas: ejecutivo y técnico.
- Estructura del reporte y narrativa de riesgo.
- Plan de remediación, priorización y retest.

Módulo 10. Cierre del curso y ruta de crecimiento

Enfoque: Aplicación práctica y siguiente paso formativo.
- Buenas prácticas para aplicar lo aprendido en un entorno real.
- Ruta de crecimiento y preparación para Level 2.

Actividades y evaluación

- Ejercicios guiados por módulo orientados a análisis de activos, amenazas e impacto.
- Revisión de evidencias mínimas y trazabilidad (documentación defendible).
- Entrega de reporte final (ejecutivo y técnico) con recomendaciones y retroalimentación.

Incluye: plantillas ROE, checklists, guía de priorización por riesgo y estructura de reporte ejecutivo/técnico.

Más información e inscripciones: csascouncil.org