

Introducción al hacking ético en laboratorio

GUÍA INTRODUCTORIA · MATERIAL EDUCATIVO



Conoce la evaluación de seguridad con prácticas educativas limitadas a laboratorios autorizados.

Nivel: Intermedio · Duración estimada del curso: 5-6 horas · Precio de catálogo: \$25 USD

Esta guía es una introducción escrita a los temas del catálogo. No equivale a un curso completo ni incluye videos. No otorga certificación oficial ni garantiza empleo.

Tus primeras herramientas

1. Principios del hacking ético

El hacking ético tiene como objetivo identificar problemas y ayudar a corregirlos. Requiere autorización expresa y un alcance definido. Tener acceso público a una web no implica permiso para probarla. Detente ante cualquier duda sobre la autorización.

2. Autorización y límites de las pruebas

Documenta qué sistemas, fechas y acciones están permitidos, así como los contactos y reglas para detener una práctica. Nunca incluyas servicios externos o cuentas reales que no estén autorizados. No realices pruebas sobre la red de tu escuela o trabajo sin permiso formal.

3. Conceptos introductorios de evaluación de seguridad

Un laboratorio local con máquinas virtuales permite aprender en un entorno controlado. Utiliza una red aislada cuando proceda y evita publicar aplicaciones vulnerables en internet. Usa datos ficticios y snapshots para poder volver a un estado conocido.

De la teoría a tus hábitos

4. Identificación de riesgos en entornos controlados

Aprende a observar configuraciones y reconocer riesgos sin afectar la disponibilidad. Prioriza comprender el problema y su mitigación. En plataformas educativas, sigue sus reglas y limita todas las actividades a los objetivos expresamente habilitados.

5. Prácticas educativas en laboratorios autorizados

Un informe básico describe el entorno autorizado, el problema observado, su posible impacto y una recomendación de corrección. No publiques datos sensibles ni explotes un hallazgo fuera del alcance. Coordina cualquier reporte con el responsable y conserva solo la información necesaria.

Ejercicio seguro

Escribe un alcance de práctica ficticio: sistema propio, acciones permitidas, límites y reglas de detención. Dibuja un laboratorio aislado sin instalar ni exponer sistemas vulnerables.

Antes de continuar

Realiza actividades únicamente en tus propias cuentas, equipos o entornos expresamente autorizados. No compartas contraseñas, códigos ni información privada. Los ajustes pueden variar según tu dispositivo o proveedor; consulta siempre su documentación oficial.