Cybersecurity Notes -- Aprendizaje Autodidacta

Este repositorio recoge mis conocimientos, notas y reflexiones dentro autodidacta y práctica.

No es un repositorio de soluciones ni writeups completos.
Es un **cuaderno técnico de aprendizaje**, centrado en metodología, conceptos y experiencia real.

🧠 Perfil general

Soy una persona autodidacta en ciberseguridad, con especial interés en entender **cómo piensa un atacante**, más allá de ejecutar herramientas sin criterio.

Mi aprendizaje se ha basado en: - Práctica constante - Entornos tipo laboratorio (como TryHackMe) - Uso real de herramientas - Reflexión sobre errores y aciertos

---

🐧 Sistema Operativo y Terminal (Linux / Kali)

Trabajo habitualmente en **Kali Linux**, utilizando el terminal como herramienta principal.

Conocimientos:

- Navegación por el sistema de archivos
- Gestión de archivos y permisos
- Procesos y servicios
- Uso de pipes y redirecciones
- Mentalidad orientada a CLI

El terminal no es solo una interfaz, es parte fundamental del flujo de trabajo en ciberseguridad.

🔍 Enumeración y Reconocimiento

La enumeración es uno de los pilares de mi aprendizaje.

Herramienta principal:

Nmap

Capacidades:

- Escaneos TCP y UDP
- Detección de servicios y versiones
- Uso de scripts NSE
- Interpretación de resultados

Entiendo que una buena enumeración: - Reduce ataques innecesarios - Marca el camino correcto - Ahorra tiempo y errores

---

Ataques de contraseñas

Conozco y he utilizado **Hydra** para ataques de credenciales en entornos controlados.

Comprensión de:

- Fuerza bruta
- Ataques por diccionario
- Importancia del servicio, contexto y diccionarios
- Limitaciones reales de este tipo de ataques

No todo se puede ni se debe atacar con fuerza bruta. El contexto manda.

Explotación

He trabajado con **Metasploit Framework** a nivel básico--intermedio.

Conocimientos:

- Búsqueda de módulos
- Configuración de opciones
- Ejecución de exploits en entornos de laboratorio

Soy consciente de que Metasploit es una herramienta potente, pero no sustituye la comprensión real de una vulnerabilidad.

Automatización y scripts

Tengo capacidad para crear **scripts con ayuda de IA**, orientados a: - Automatizar tareas repetitivas - Organizar resultados - Facilitar la enumeración

Aunque no soy programador clásico, entiendo la lógica y el propósito de la automatización dentro del hacking.

Redes y fundamentos teóricos

Poseo conocimientos básicos de: - Redes - Protocolos - Puertos - Relación entre servicios y vectores de ataque

Estos fundamentos me permiten entender **por qué** un puerto abierto o un servicio expuesto puede ser relevante.

Filosofía de aprendizaje

No busco: - Memorizar comandos sin entenderlos - Copiar soluciones - Acumular certificaciones sin base

Busco: - Comprender procesos - Aprender de los errores - Pensar como atacante - Construir conocimiento sólido paso a paso

⚠ Nota ética

Este repositorio: - ❌ No contiene flags - ❌ No contiene soluciones completas - ❌ No viola términos de plataformas de aprendizaje

Todo el contenido es educativo y reflexivo.

📌 Objetivo del repositorio

- Consolidar conocimientos
- Documentar aprendizaje
- Mejorar metodología
- Compartir una visión honesta del proceso de aprendizaje en ciberseguridad

🔄 En progreso

Este repositorio está vivo y seguirá creciendo a medida que: - Aprenda nuevas técnicas - Profundice en explotación - Mejore mis scripts - Refuerce conceptos de red y web hacking