🛠️ Ejercicio Práctico – Nivel Medio

📌 **Título:** Escaneo y Explotación de una Máquina Vulnerable con Kali Linux y Vulnhub

---

🎯 Objetivo del ejercicio:

Simular una auditoría de seguridad en una máquina vulnerable importada desde **Vulnhub**, utilizando herramientas ofensivas desde **Kali Linux**. Aprenderás a identificar servicios expuestos, buscar vulnerabilidades conocidas y ejecutar una explotación básica de forma controlada.

📝 Escenario:

Has descargado e importado una máquina vulnerable desde **https://www.vulnhub.com** (por ejemplo, *"Mr. Robot: 1"*, *"Metasploitable2"* o *"Basic Pentesting 1"*). Tu tarea consiste en escanearla desde Kali Linux, identificar los servicios disponibles y demostrar una vulnerabilidad real de forma ética y segura.

🔍 Tu tarea:

✅ Paso 1 – Configuración del entorno

1. Importa la VM descargada desde Vulnhub a VirtualBox.
2. Configura la red de ambas máquinas (Kali Linux y la VM vulnerable) en modo **"Solo Anfitrión"** o **"Red Interna"**.
3. Inicia ambas máquinas y verifica su conectividad usando el comando:

ping <IP de la máquina vulnerable>

✅ Paso 2 – Escaneo de servicios con Nmap

1. Identifica la dirección IP de la máquina vulnerable.
2. Ejecuta un escaneo con:

nmap -sS -sV -O <IP objetivo>

3. Registra:
    - Puertos abiertos
    - Servicios disponibles
    - Versiones de software detectadas

✅ Paso 3 – Análisis de vulnerabilidades

1. Selecciona uno de los servicios encontrados.
2. Busca una vulnerabilidad conocida (CVE) para ese servicio usando:
    - Google + versión del servicio
    - https://cvedetails.com
    - https://exploit-db.com
3. Documenta:
    - Nombre del servicio
    - Número de versión
    - Vulnerabilidad (CVE)
    - Descripción del fallo

✅ Paso 4 – Simulación de explotación

1. Usa una herramienta ofensiva para simular la explotación:
    - `Metasploit Framework`
    - `sqlmap`
    - `Hydra`
    - `Netcat` (dependiendo del servicio expuesto)
2. Demuestra una acción concreta:
    - Obtener acceso no autorizado
    - Enumerar usuarios
    - Ejecutar comandos remotos
    - Ver archivos de sistema
3. Registra los comandos utilizados y capturas de salida.

✅ Paso 5 – Recomendaciones de remediación

1. Describe los riesgos del fallo encontrado.
2. Escribe **tres recomendaciones técnicas** que podrían corregir la vulnerabilidad explotada.
3. Redacta un párrafo de reflexión ética sobre el uso responsable de estas herramientas.

🧪 Resultado esperado:

- Escaneo completo y documentado
- CVE identificada correctamente
- Simulación de explotación ejecutada con éxito

- Capturas de pantalla o comandos guardados
- Informe con recomendaciones y reflexión final

🧠 Reflexión Final:

¿Qué técnicas aprendiste en este ejercicio?
¿Qué importancia tiene la documentación durante un pentest?
¿Cómo contribuye esta práctica a tu desarrollo como profesional ético en ciberseguridad?
