




Ejercicio Práctico

 **Título:** Análisis de Seguridad y Validación de Vulnerabilidades con Pruebas Controladas

Objetivo del ejercicio:

Aplicar las fases iniciales y centrales de un pentest (reconocimiento, escaneo, explotación básica), interpretando vulnerabilidades en un entorno controlado y documentando los hallazgos mediante capturas o registros técnicos.

Escenario:

Formas parte del equipo de ciberseguridad de una empresa ficticia. Te asignaron evaluar un servidor de pruebas con dirección IP **192.168.1.150**. Tu labor es ejecutar un análisis de seguridad estructurado que incluya:

- Recolección de información pública
 - Escaneo activo de puertos y servicios
 - Validación básica de una vulnerabilidad explotable sin comprometer el sistema
 - Documentación del hallazgo y propuesta de remediación
-

Tu tarea:

Paso 1 – Reconocimiento y mapeo inicial

1. Utiliza herramientas como:
 - **whois**, **nslookup**, **dig** para simular análisis DNS

- **Shodan** o **Censys** (simulado) para identificar exposición pública

2. Documenta:

- Servicios encontrados
- Tecnologías visibles (servidor web, CMS, etc.)
- Posibles rutas sensibles (**/admin**, **/login**, **/backup**, etc.)

✓ Paso 2 – Escaneo de puertos y servicios

Ejecuta un escaneo completo sobre el host objetivo:

```
nmap -sS -sV -T4 -p- 192.168.1.150
```

- 1.
2. Identifica:
 - Puertos abiertos
 - Versiones de software
 - Servicios vulnerables

 *Anota al menos 2 servicios que puedan ser objetivo de análisis.*

✓ Paso 3 – Búsqueda de vulnerabilidades conocidas

1. Para los servicios detectados, busca CVEs (por ejemplo, en <https://cve.mitre.org/> o [ExploitDB](#))
2. Selecciona **una vulnerabilidad reproducible** de bajo riesgo para demostrar el impacto potencial
3. Documenta:
 - Nombre de la vulnerabilidad (CVE)
 - Servicio afectado
 - Comando o script simulado utilizado para probarla (sin causar daño)

✓ Paso 4 – Simulación de explotación segura

1. Usa herramientas como **Nikto**, **Sqlmap**, **Metasploit** o scripts de prueba para demostrar la vulnerabilidad
 - Ejemplo: `sqlmap -u "http://192.168.1.150/products.php?id=1" --dbs`
2. Captura evidencias (respuestas del sistema, códigos de error, bases de datos listadas, etc.)

 Incluye capturas o comandos empleados para mostrar la simulación.

✓ Paso 5 – Reporte técnico y recomendaciones

1. Redacta un mini-informe que incluya:
 - Descripción de la vulnerabilidad explotada
 - Riesgo potencial (alto, medio, bajo)
 - Recomendaciones para mitigarla (actualización, refuerzo de autenticación, cierre de puertos, etc.)
 2. Agrega una reflexión personal sobre lo aprendido
-

Resultado esperado:

- Bitácora técnica con comandos usados
 - Evidencias documentadas (capturas, logs, análisis)
 - Informe con recomendación de remediación
 - Conciencia ética durante todo el proceso
-

Reflexión Final:

¿Qué dificultades encontraste al buscar vulnerabilidades?

¿Cómo evalúas la importancia de documentar de forma profesional los hallazgos?

¿Qué aprendiste sobre la gestión del riesgo en la práctica?
