




Ejercicio Práctico

 **Título:** Auditoría Ética y Documentación de Vulnerabilidades en un Entorno de Pruebas Controlado

Objetivo general:

Simular una prueba de penetración completa utilizando una máquina vulnerable, aplicando técnicas de reconocimiento, escaneo, explotación básica y documentación profesional de los hallazgos, siguiendo metodologías estándar (OWASP y PTES).

Escenario:

Tu equipo de auditoría ha recibido autorización para evaluar la seguridad de una aplicación vulnerable desplegada en un entorno de laboratorio. El cliente necesita un informe profesional que documente hallazgos reales, riesgos y recomendaciones.

Tienes acceso a una máquina virtual vulnerable (como **DVWA**, **Metasploitable2** o una instancia de **TryHackMe/VulnHub**) y deberás identificar al menos **una vulnerabilidad explorable**, validarla manualmente y documentarla.

Fase 1 – Reconocimiento

1. Realiza un reconocimiento activo y pasivo de la máquina objetivo.
2. Usa herramientas como:
 - `nslookup`, `dig`, `whois`, `theHarvester`, `Shodan`, etc.

Entrega: Breve resumen con lo que descubriste del dominio/IP (tecnologías, servicios, DNS, puertos, etc.).

✓ Fase 2 – Escaneo de servicios y vulnerabilidades

1. Utiliza `nmap -sS -sV -O` y `--script=vuln` para escanear la máquina.
2. Identifica puertos abiertos, versiones y posibles vulnerabilidades.

Entrega: Captura o reporte resumido con los servicios detectados y al menos una vulnerabilidad aparente.

✓ Fase 3 – Explotación controlada

1. Elige una vulnerabilidad y explótala manualmente (ej: SQLi, XSS, CSRF) o con ayuda de herramientas como Burp Suite, Sqlmap o Metasploit.
2. No uses ataques destructivos. Solo demuestra el impacto con evidencia controlada.

Entrega:

- Capturas de pantalla del exploit
 - Descripción del comportamiento observado
 - Impacto estimado
-

✓ Fase 4 – Documentación técnica del hallazgo

Redacta un informe profesional que contenga:

1. Título del hallazgo
 2. Descripción técnica del problema
 3. Evidencia técnica (comandos, payloads, capturas)
 4. Evaluación del impacto y nivel de riesgo
 5. Recomendaciones técnicas para mitigar la vulnerabilidad
 6. Referencias (OWASP, CVSS, etc.)
-

✓ Fase 5 – Cierre ético y reflexión

Redacta un breve párrafo final explicando:

- Por qué es importante **documentar de forma clara y ética**
 - Cómo este ejercicio te ayudó a **comprender el ciclo completo de un pentest**
-

Criterios de Evaluación (máximo 10 puntos)

1. **Reconocimiento y escaneo bien ejecutado (2 pts)**
Identificación precisa de puertos, servicios y posibles vulnerabilidades.
 2. **Explotación controlada y ética (2 pts)**
Se demuestra el impacto de una vulnerabilidad sin afectar la estabilidad del sistema.
 3. **Calidad del hallazgo documentado (2 pts)**
El informe incluye título, evidencia, análisis de impacto y referencias claras.
 4. **Recomendaciones técnicas (1.5 pts)**
Propuestas claras, realistas y bien fundamentadas para mitigar la vulnerabilidad.
 5. **Reflexión ética (1 pt)**
Se comprende la importancia del rol ético y responsable del auditor.
 6. **Presentación y redacción del informe (1.5 pts)**
Informe profesional, claro, coherente y bien estructurado.
-

Recursos de Apoyo y Documentación Sugerida

Herramientas de Reconocimiento y Escaneo

- [nslookup](#), [dig](#): Consulta DNS.
- [theHarvester](#): Recolección de correos, subdominios, hosts.
- [Shodan](#): Motor de búsqueda para dispositivos conectados.
- [nmap](#): Escaneo de puertos y scripts de vulnerabilidades.
- [Sqlmap](#): Automatización de pruebas SQLi.
- [Burp Suite](#): Análisis e interceptación de tráfico web.

- [Metasploit](#): Framework de explotación.

Entornos Seguros de Prueba

- [Metasploitable2](#)
- [DVWA – Damn Vulnerable Web Application](#)
- [TryHackMe](#)
- [VulnHub](#)

Lecturas Recomendadas

- [OWASP Testing Guide](#)
- [PTES – Penetration Testing Execution Standard](#)
- [CVSS – Common Vulnerability Scoring System](#)

Reflexión Final

“Una auditoría ética no solo mide vulnerabilidades técnicas, sino también la madurez profesional del auditor. La capacidad de reconocer, documentar y comunicar hallazgos con responsabilidad es tan importante como encontrar fallos.”
