



Ejercicio Práctico

 **Título:** Simulación de un Reconocimiento y Escaneo de Seguridad Controlado

Objetivo del ejercicio:

Familiarizarse con las dos primeras fases de una prueba de penetración: **Reconocimiento** y **Escaneo**, utilizando herramientas comunes en entornos seguros y simulados. El estudiante aplicará técnicas básicas de recopilación de información y escaneo técnico para identificar puertos abiertos y servicios activos en un objetivo de prueba.


Escenario:

Te han asignado la tarea de evaluar el nivel básico de seguridad de un servidor de pruebas dentro de una red interna segura. Se te ha proporcionado acceso a una máquina virtual o entorno simulado (como Metasploitable, TryHackMe o Hack The Box). Tu responsabilidad es realizar reconocimiento pasivo y escaneo activo sobre un objetivo específico.

Tu tarea:


Paso 1 – Reconocimiento (OSINT básico):

1. Simula la búsqueda de información pública sobre el dominio objetivo `example.local`.
2. Utiliza herramientas como `whois`, `nslookup`, y `Google Dorking` para identificar:
 - Información de registros DNS
 - Tecnología de servidores web
 - Posibles usuarios o empleados relacionados

 *Registra los resultados obtenidos en un archivo de texto o en tu bitácora personal.*

Paso 2 – Escaneo de puertos y servicios:

1. Ejecuta un escaneo básico con Nmap al objetivo **192.168.1.100**.
 - Comando recomendado: **nmap -sS -sV 192.168.1.100**
2. Identifica:
 - Puertos abiertos
 - Servicios activos
 - Versiones de software encontradas

 *Anota cuáles servicios podrían representar un riesgo potencial si no están actualizados.*

Paso 3 – Análisis básico:

1. Analiza los resultados del escaneo y responde:
 - ¿Qué puertos están abiertos?
 - ¿Qué servicios están en ejecución?
 - ¿Alguno está desactualizado o vulnerable?
2. Investiga uno de los servicios encontrados y determina si tiene vulnerabilidades conocidas (puedes usar CVE o Exploit-DB).

Paso 4 – Recomendaciones:

Escribe una breve recomendación de seguridad (3 a 5 líneas) para mitigar los riesgos observados.

 **Resultado esperado:**

- Bitácora con resultados del reconocimiento y escaneo
 - Identificación de al menos 2 servicios vulnerables o desactualizados
 - Recomendación clara para reforzar la seguridad del sistema
-

Reflexión Final:

- ¿Qué aprendiste sobre la importancia de las fases iniciales del pentesting?
 - ¿Cómo puede el reconocimiento pasivo revelar información crítica?
-

Solución – Ejercicio Práctico

Simulación de un Reconocimiento y Escaneo de Seguridad Controlado

Objetivo cumplido:

Se realizó la fase de reconocimiento con herramientas OSINT básicas y el escaneo activo del host de pruebas. Se identificaron puertos abiertos y servicios vulnerables, y se propusieron recomendaciones para mitigar riesgos.

Paso 1 – Reconocimiento (OSINT básico)

- Dominio objetivo: `example.local`
- Herramientas utilizadas:
 - `whois example.local` → *Dominio ficticio, no registrado públicamente*
 - `nslookup example.local` → *Simula que apunta a 192.168.1.100*
 - Búsqueda en Google: `site:example.local`
→ Resultado simulado: se identificó un panel de login en `http://example.local/admin`

Hallazgos:

- El sitio utiliza Apache 2.4.29 (expresado en el footer del sitio)
 - La ruta `/admin` podría ser un vector de entrada si no está protegida
-

✓ Paso 2 – Escaneo de puertos y servicios

Comando ejecutado:

```
nmap -sS -sV 192.168.1.100
```

Resultado (simulado):

Puerto	Servicio	Versión detectada
22	SSH	OpenSSH 7.2p2
80	HTTP	Apache 2.4.29
3306	MySQL	MySQL 5.7.20

✓ Paso 3 – Análisis básico

Observaciones:

- Apache 2.4.29 tiene reportadas múltiples vulnerabilidades, incluyendo CVE-2017-15715
 - MySQL 5.7.20 es una versión desactualizada con vulnerabilidades como CVE-2018-2562
 - El puerto 22 (SSH) expuesto podría ser blanco de fuerza bruta si no hay autenticación robusta
-

✓ Paso 4 – Recomendaciones

- **Actualizar Apache** a una versión más reciente que corrija vulnerabilidades conocidas.
- **Restringir el acceso a SSH** mediante firewall o listas de control de acceso (ACL).

- **Auditar MySQL** y actualizar a una versión estable sin vulnerabilidades públicas.
 - **Ocultar rutas sensibles** como `/admin` mediante autenticación fuerte y medidas de seguridad (por ejemplo, MFA o firewall de aplicaciones web).
-

Reflexión Final

Este ejercicio me permitió comprender el valor del reconocimiento pasivo y el escaneo controlado como fases esenciales del pentesting.

Aprendí a identificar servicios expuestos y reconocer riesgos a partir de versiones desactualizadas.

Esta metodología me ayudará a evaluar entornos reales con una mentalidad preventiva.
