🛠️ Ejercicio Práctico

📌 **Título:** Reconocimiento y Escaneo de Puertos Básico con Nmap

---

🎯 Objetivo del ejercicio:

Familiarizarse con el proceso de **reconocimiento** pasivo y **escaneo de puertos** utilizando **Nmap** para detectar servicios y puertos abiertos en un objetivo controlado, aprendiendo a interpretar los resultados y aplicando buenas prácticas de seguridad.

📝 Escenario:

Estás trabajando en un entorno de pruebas de ciberseguridad. Te han asignado una máquina virtual vulnerable para identificar los puertos abiertos y servicios en ejecución. Para esto, utilizarás **Kali Linux** y **Nmap**. El objetivo es realizar un escaneo básico sin interactuar directamente con el sistema objetivo.

🔍 Tu tarea:

✅ Paso 1 – Configuración del entorno

1. Asegúrate de tener **Kali Linux** instalado y en funcionamiento.
2. Descarga una **máquina vulnerable de Vulnhub** (por ejemplo, **Metasploitable2** o **Basic Pentesting 1**).
3. Configura la red en **modo "Solo Anfitrión"** en **VirtualBox** o **VMware** para aislar las máquinas.
4. Inicia la máquina vulnerable y verifica su dirección IP utilizando:

ifconfig

✅ Paso 2 – Escaneo de puertos con Nmap

1. Abre la terminal en **Kali Linux** y ejecuta un escaneo básico de puertos en la dirección IP de la máquina vulnerable:

nmap -sS <IP de la máquina vulnerable>

2. Registra los puertos abiertos que aparezcan en el resultado.

✅ Paso 3 – Escaneo de versiones de servicios

1. Ejecuta un escaneo de versiones de servicios para identificar software y versiones en ejecución:

nmap -sV <IP de la máquina vulnerable>

2. Anota las versiones de los servicios encontrados.

✅ Paso 4 – Investigación de vulnerabilidades

1. Basándote en los servicios y versiones detectadas, realiza una búsqueda rápida en Internet sobre vulnerabilidades conocidas (CVE) para los servicios identificados.

2. Documenta cualquier vulnerabilidad que encuentres relacionada con los servicios detectados (puedes utilizar fuentes como **CVE Details** o **Exploit-DB**).

✅ Paso 5 – Reflexión y recomendaciones

1. Reflexiona sobre los resultados obtenidos:
    - ¿Qué puertos y servicios fueron encontrados?
    - ¿Qué vulnerabilidades conocidas pueden ser explotadas?

2. Redacta **tres recomendaciones básicas** para mitigar los riesgos asociados con los servicios expuestos.

🧪 Resultado esperado:

- Un escaneo básico de puertos utilizando Nmap
- Identificación de servicios en ejecución y sus versiones
- Investigación de vulnerabilidades asociadas a esos servicios
- Recomendaciones sobre cómo mitigar los riesgos

🧠 Reflexión Final:

¿Qué aprendiste sobre el proceso de escaneo de puertos y servicios?
¿Por qué es importante identificar las versiones de los servicios en ejecución?
¿Cómo puedes proteger un sistema expuesto a ataques?

🛠️ Solución – Ejercicio Práctico

📌 Reconocimiento y Escaneo de Puertos Básico con Nmap

🎯 Objetivo cumplido:

Se logró realizar un escaneo de puertos y detección de servicios desde Kali Linux hacia una máquina vulnerable configurada en red aislada. Se interpretaron correctamente los resultados y se propusieron medidas básicas de mitigación.

✅ Paso 1 – Configuración del entorno

Máquinas utilizadas:

- Kali Linux (host de ataque)

- Metasploitable2 (máquina vulnerable)

Configuración de red:

- Modo “Solo Anfitrión” en VirtualBox

Dirección IP obtenida (Metasploitable2):

192.168.56.101

✅ Conectividad verificada vía ping.

✅ Paso 2 – Escaneo de puertos con Nmap

Comando ejecutado:

nmap -sS 192.168.56.101

Resultado parcial:

```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
```

✅ Se detectaron múltiples puertos abiertos, entre ellos servicios comunes con historial de vulnerabilidades.

✅ Paso 3 – Escaneo de versiones

Comando ejecutado:

nmap -sV 192.168.56.101

Resultado parcial:

21/tcp vsftpd 2.3.4
22/tcp OpenSSH 4.7p1 Debian
23/tcp Linux telnetd
80/tcp Apache httpd 2.2.8
3306/tcp MySQL 5.0.51a

✅ Versiones detectadas correctamente.

✅ Paso 4 – Investigación de vulnerabilidades

Servicio vulnerable seleccionado:
vsftpd 2.3.4

CVE relevante:
CVE-2011-2523 – *Backdoor en versión 2.3.4 de vsftpd*

Descripción breve:
Esta versión permite una conexión de shell remota al conectarse al puerto FTP con un nombre de usuario especial que contiene ":)".

✅ Paso 5 – Recomendaciones

Servicios detectados:

- FTP, Telnet, HTTP, SSH, NetBIOS, MySQL

Riesgos detectados:

- Uso de protocolos inseguros como Telnet y FTP
- Servicios desactualizados con vulnerabilidades públicas conocidas

Recomendaciones:

1. **Actualizar vsftpd y otros servicios a versiones seguras.**
2. **Deshabilitar servicios innecesarios como Telnet o NetBIOS.**
3. **Implementar reglas de firewall para limitar el acceso externo a puertos sensibles.**

🧠 Reflexión Final

Este ejercicio permitió comprender cómo **Nmap puede detectar información crítica** sobre sistemas vulnerables. Identificar puertos abiertos y versiones de servicios ayuda a anticiparse a ataques.
La interpretación de estos datos es esencial para emitir recomendaciones de seguridad efectivas.
Trabajar en entornos aislados proporciona una experiencia segura, controlada y ética.
