Ejercicio de Reconocimiento y Escaneo de Puertos con Nmap

Objetivo del ejercicio

El propósito de este ejercicio es adquirir dominio sobre el uso de Nmap para realizar tareas de reconocimiento pasivo, escaneo de puertos y enumeración de servicios sobre un sistema objetivo dentro de un entorno controlado de ciberseguridad. A través del escaneo y análisis de puertos, se pretende identificar qué servicios están expuestos, determinar sus versiones, y detectar posibles vectores de ataque asociados.

Configuración inicial del entorno

El primer paso consiste en preparar un entorno seguro para realizar las pruebas. Para ello, se requiere disponer de:

- **Kali Linux** como sistema de análisis (máquina atacante).
- **Una máquina vulnerable** descargada desde https://vulnhub.com, como *Metasploitable2* o *Basic Pentesting 1*.
- Configuración de red en **modo "Solo Anfitrión" (Host-only)** dentro de VirtualBox o VMware, para garantizar aislamiento de la red externa y evitar interferencias.

Una vez iniciadas ambas máquinas, se debe obtener la dirección IP de la víctima mediante el comando:

```
ifconfig
```

Esto devolverá la IP asignada (por ejemplo, `192.168.56.101`). Se recomienda verificar conectividad desde Kali con:

```
ping 192.168.56.101
```

Escaneo de puertos con Nmap (descubrimiento de superficie expuesta)

Con la IP ya identificada, se procede a realizar un **escaneo básico de puertos TCP**, empleando el comando:

nmap -sS 192.168.56.101

La opción `-sS` ejecuta un escaneo SYN (“stealth”), enviando paquetes SYN sin completar la conexión TCP. Esto permite detectar puertos abiertos con menor probabilidad de ser detectado por mecanismos de defensa.

Ejemplo de resultados esperados:

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

Aquí observamos múltiples servicios comunes habilitados, lo que sugiere una superficie de ataque considerable.

Detección de versiones de servicios

El siguiente paso consiste en determinar con precisión qué versiones de software están corriendo en los puertos identificados. Para ello se utiliza:

nmap -sV 192.168.56.101

El parámetro `-sV` activa la detección de versiones mediante banners, firmas y algoritmos de fingerprinting.

Ejemplo de resultados:

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

Este resultado es clave para el análisis posterior de vulnerabilidades. Versiones antiguas como `vsftpd 2.3.4` y `Apache 2.2.8` son conocidas por contener fallos críticos ampliamente documentados.

Investigación de vulnerabilidades (análisis contextual del riesgo)

Con las versiones identificadas, se realiza una investigación técnica para buscar vulnerabilidades conocidas (CVE) asociadas a cada servicio. Para esto se pueden utilizar fuentes como:

- https://cvedetails.com
- https://nvd.nist.gov
- https://exploit-db.com

Por ejemplo, se detecta que el servicio FTP corre `vsftpd 2.3.4`, el cual está asociado a una **vulnerabilidad crítica**:

- **CVE-2011-2523**
  Esta versión contiene un *backdoor* que permite obtener una shell remota al enviar un nombre de usuario especial que contenga `:)`.

Asimismo, versiones antiguas de Apache y MySQL también presentan múltiples CVEs relacionadas con inyecciones, ejecución remota de código, y fugas de información.

Análisis de riesgos

Basado en la información recolectada, se concluye que el sistema objetivo tiene múltiples puntos débiles:

- Exposición de **protocolos inseguros** (Telnet y FTP).

- Presencia de **software obsoleto y vulnerable**.

- **Puertos críticos accesibles sin restricción** desde cualquier host dentro de la red aislada.

Estas condiciones lo convierten en un blanco ideal para pruebas de penetración, explotación de vulnerabilidades o escalamiento de privilegios.

Recomendaciones de mitigación

Para reducir el riesgo asociado, se sugieren las siguientes medidas técnicas:

1. **Actualizar los servicios** a versiones estables y soportadas (especialmente vsftpd, Apache, y MySQL).

2. **Deshabilitar servicios innecesarios** como Telnet y NetBIOS, que no deberían estar activos en entornos modernos.

3. **Configurar un firewall local** o de red que limite el acceso externo a los puertos expuestos solo a direcciones IP autorizadas.