Simulación y Resolución del Laboratorio de Nmap

Este recorrido simulado te guiará a través de cada paso, asumiendo que tienes Nmap instalado y una dirección IP de destino (por ejemplo, 192.168.1.100 para una máquina vulnerable hipotética o un dispositivo en tu red que tengas permiso para escanear).

Preparación del Entorno

Primero, asegúrate de que Nmap esté instalado. Si estás en un sistema basado en Debian (como Ubuntu o Kali Linux), abre tu terminal y ejecuta:

Bash

sudo apt install nmap

También necesitarás un objetivo. Para este laboratorio, asumamos que tu dirección IP de destino es 192.168.1.100. Si estás usando una máquina virtual, puedes configurar su IP para que esté en la misma subred que tu host o usar una red donde ambas máquinas puedan comunicarse.

Paso 1: Escaneo Básico de Host

Este paso te ayuda a descubrir dispositivos activos en tu red.

- **Comando que ejecutarías:**

Bash

nmap -sn 192.168.1.0/24

- **Salida esperada:** Verías una lista de hosts que están activos y responden a solicitudes de ping dentro de la subred 192.168.1.0/24. Podría verse algo como esto:
- Starting Nmap 7.91 (https://nmap.org) at 2025-05-20 18:30 CDT
- Nmap scan report for 192.168.1.1
- Host is up (0.00020s latency).
- Nmap scan report for 192.168.1.100
- Host is up (0.00035s latency).

- Nmap scan report for 192.168.1.200
- Host is up (0.00040s latency).
- Nmap done: 256 IP addresses (3 hosts up) scanned in 2.12 seconds

Resolución: Identifica la **dirección IP de tu dispositivo de destino** (por ejemplo, 192.168.1.100) a partir de esta salida.

Paso 2: Escaneo de Puertos y Servicios

Ahora, escanearás tu objetivo en busca de puertos abiertos.

- **Comando que ejecutarías:**

Bash

nmap -sS 192.168.1.100

- **Salida esperada:** Nmap realizará un escaneo SYN y listará los puertos abiertos.
- Starting Nmap 7.91 (https://nmap.org) at 2025-05-20 18:32 CDT
- Nmap scan report for 192.168.1.100
- Host is up (0.00030s latency).
- Not shown: 996 closed ports
- PORT STATE SERVICE
- 22/tcp open ssh
- 80/tcp open http
- 443/tcp open https
- 3389/tcp open ms-wbt-server
-
- Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds

Resolución: Anota los **puertos abiertos** y sus **servicios asociados**. En este ejemplo, los puertos 22 (SSH), 80 (HTTP), 443 (HTTPS) y 3389 (MS-WBT-Server) están abiertos.

Paso 3: Detección de Versión de Servicios

Este paso te ayuda a recopilar información más específica sobre la versión de los servicios que se ejecutan en los puertos abiertos.

- **Comando que ejecutarías:**

Bash

nmap -sV 192.168.1.100

- **Salida esperada:** Verás el nombre del servicio, la versión y, potencialmente, el sistema operativo que ejecuta ese servicio.
- Starting Nmap 7.91 (https://nmap.org) at 2025-05-20 18:34 CDT
- Nmap scan report for 192.168.1.100
- Host is up (0.00030s latency).
- Not shown: 996 closed ports
- PORT STATE SERVICE VERSION
- 22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.1
- 80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
- 443/tcp open ssl/http Apache httpd 2.4.41 ((Ubuntu))
- 3389/tcp open ms-wbt-server?
-
- Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
- Nmap done: 1 IP address (1 host up) scanned in 5.23 seconds

Resolución: Identifica las **versiones específicas** de los servicios. Por ejemplo, aquí se identifican OpenSSH 8.2p1 y Apache httpd 2.4.41. Estas versiones pueden cotejarse posteriormente con bases de datos de vulnerabilidades.

Paso 4: Escaneo de Sistema Operativo (OS)

Esto ayuda a identificar el sistema operativo del host de destino.

- **Comando que ejecutarías:**

Bash

nmap -O 192.168.1.100

- **Salida esperada:** Nmap intentará identificar el sistema operativo.
- Starting Nmap 7.91 (https://nmap.org) at 2025-05-20 18:36 CDT
- Nmap scan report for 192.168.1.100
- Host is up (0.00030s latency).
- Not shown: 996 closed ports
- PORT   STATE SERVICE
- 22/tcp   open ssh
- 80/tcp   open http
- 443/tcp open https

3389/tcp open ms-wbt-server Device type: general purpose Running: Linux 4.X|5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 6.78 seconds

```

**Resolución:** Determina el **sistema operativo**. En este ejemplo, se identifica como Linux 4.x|5.x. Esta información es crucial para comprender las posibles vulnerabilidades a nivel del sistema operativo.

---

**Paso 5: Escaneo Completo con Scripts de Nmap (Detección de Vulnerabilidades)**

Esto aprovecha el motor de scripts de Nmap para encontrar vulnerabilidades comunes.

- **Comando que ejecutarías:**

Bash
```

nmap --script vuln 192.168.1.100

- **Salida esperada:** Esta salida puede ser extensa. Nmap ejecutará varios scripts de vulnerabilidad. Podrías ver advertencias sobre posibles exploits, configuraciones erróneas o vulnerabilidades conocidas para los servicios detectados.
- Starting Nmap 7.91 (https://nmap.org) at 2025-05-20 18:38 CDT
- Nmap scan report for 192.168.1.100
- Host is up (0.00030s latency).
- Not shown: 996 closed ports
- PORT STATE SERVICE
- 22/tcp open ssh
- | ssh-hostkey:
- | 3072 c8:b3:f1:40:99:9f:dd:16:a2:e0:1a:06:d2:4b:20:9b (RSA)
- |_ 256 ee:ea:2c:0b:3e:7b:7c:b8:e2:f8:8b:04:1e:a9:d2:d7 (ECDSA)
- 80/tcp open http
- | http-server-header: Apache/2.4.41 (Ubuntu)
- | http-methods:
- |_ Potentially risky methods: TRACE
- 443/tcp open https
- | http-server-header: Apache/2.4.41 (Ubuntu)
- | http-methods:
- |_ Potentially risky methods: TRACE
- |_ssl-date: TLS randomness does not represent time
- 3389/tcp open ms-wbt-server?
- Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
-
- Nmap done: 1 IP address (1 host up) scanned in 15.67 seconds

Resolución: Analiza la salida cuidadosamente. Busca cualquier sección que indique "VULNERABLE" o que resalte debilidades específicas. Por ejemplo, si http-methods muestra TRACE como un método potencialmente riesgoso, sugiere una vulnerabilidad del método TRACE.

Paso 6: Generar un Informe de Resultados

Guardar tus resultados es esencial para la documentación.

- **Comando que ejecutarías:**

Bash

nmap -sV -O -oN resultados_nmap.txt 192.168.1.100

- **Salida esperada:** Nmap realizará la detección de versión y SO y luego guardará toda la salida en un archivo llamado resultados_nmap.txt en el directorio donde ejecutaste el comando. No verás la salida directamente en la terminal, sino un mensaje que confirma el escaneo y el guardado del archivo.
- Starting Nmap 7.91 (https://nmap.org) at 2025-05-20 18:45 CDT
- Nmap scan report for 192.168.1.100
- Host is up (0.00030s latency).
- ... (detalles del escaneo) ...
- Nmap done: 1 IP address (1 host up) scanned in 8.12 seconds

Resolución: Verifica que el archivo fue creado listando el contenido del directorio (ls o dir). Abre resultados_nmap.txt con un editor de texto para revisar la información del escaneo guardada. Este archivo sirve como tu **informe**.

Paso 7: Escaneo de Vulnerabilidades Específicas

Dirigirse a vulnerabilidades específicas puede darte una imagen más detallada.

- **Comando que ejecutarías:**

Bash

nmap --script ssl-enum-ciphers -p 443 192.168.1.100

- **Salida esperada:** Este script intentará enumerar los cifrados SSL/TLS admitidos en el puerto 443.
- Starting Nmap 7.91 (https://nmap.org) at 2025-05-20 18:48 CDT
- Nmap scan report for 192.168.1.100
- Host is up (0.00030s latency).
- PORT   STATE SERVICE
- 443/tcp open https
- | ssl-enum-ciphers:
- | TLSv1.0:
- | ciphers:
- | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
- | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
- | compressors:
- | NULL
- | cipher preference: server
- | warnings:
- | Weak certificate or key.
- | TLSv1.2:
- | ciphers:
- | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
- | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
- | compressors:
- | NULL
- |_ least strength: A
- Nmap done: 1 IP address (1 host up) scanned in 7.89 seconds

Resolución: Examina la lista de cifrados y cualquier **advertencia**. En este ejemplo, la advertencia "Weak certificate or key" indica una posible vulnerabilidad. Idealmente, querrás ver cifrados fuertes y sin advertencias.