Práctica de Exploración de Red con Nmap

1. Preparar el entorno e instalar Nmap

compose.yml

```yaml
services:
  apache:
    image: httpd:latest
    container_name: apache-container
    ports:
      - "80:80"
    networks:
      - my-network

  ubuntu:
    image: ubuntu:latest
    container_name: ubuntu-container
    command: sleep infinity
    networks:
      - my-network
    tty: true
    stdin_open: true

networks:
  my-network:
    driver: bridge
```

Instalación de Nmap

```
# nmap -p 80 apache-container
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-18 21:54 UTC
Nmap scan report for apache-container (172.21.0.2)
Host is up (0.000040s latency).
rDNS record for 172.21.0.2: apache-container.tarea1_my-network

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:42:AC:15:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

2. Mapeo de red básico

```
# nmap -sn 172.18.0.0/16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-18 21:56 UTC
Nmap scan report for 172.18.0.1
Host is up (0.00011s latency)
```

3. Mapeo con ping

```
# nmap -sn 192.168.1.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2025-02-18 22:21 UTC
Nmap scan report for 192.168.1.0
Host is up (0.00043s latency).
Nmap scan report for 192.168.1.1
Host is up (0.0021s latency).
Nmap scan report for 192.168.1.2
Host is up (0.0014s latency).
...
Nmap scan report for 192.168.1.255
Host is up (0.00051s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 21.37 seconds
```

4. Mapeo de puertos específicos

```
# nmap -sn -T4 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-18 22:25 UTC
Nmap scan report for 192.168.1.0
Host is up (0.0010s latency).
Nmap scan report for 192.168.1.1
Host is up (0.00099s latency).
Nmap scan report for 192.168.1.2
Host is up (0.00073s latency)
Nmap scan report for 192.168.1.255
Host is up (0.00061s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 17.86 seconds
```

5. Detección de versiones

```
# nmap -sV 192.168.1.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-18 22:27 UTC
Nmap scan report for 192.168.1.5
Host is up (0.00062s latency).
All 1000 scanned ports on 192.168.1.5 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.49 seconds
```

6. Huella digital del sistema operativo

```
# nmap -O 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-18 22:27 UTC
Warning: 192.168.1.33 giving up on port because retransmission cap hit
(10).
```

7. Escaneo de puertos TCP y UDP

Escaneo TCP:

```
# nmap -sT 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-18 22:29 UTC
Nmap scan report for 192.168.1.0
Host is up (0.00052s latency).
All 1000 scanned ports on 192.168.1.0 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
```

Escaneo UDP:

```
# nmap -sU -F 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-18 22:29 UT
```

8. Escaneo SYN (Sigiloso)

```
# nmap -sS 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-18 22:31 UTC
Nmap scan report for 192.168.1.0
Host is up (0.00031s latency).
All 1000 scanned ports on 192.168.1.0 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response
```

9. Scripts de auditoría de seguridad

```
# nmap -sV --script vulners 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-18 22:31 UTC

Warning: 192.168.1.33 giving up on port because retransmission cap hit(10)
```

📎 Anexo: Obtener la dirección de red en Ubuntu

```
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.21.0.3  netmask 255.255.0.0  broadcast 172.21.255.255
        ether 02:42:ac:15:00:03  txqueuelen 0  (Ethernet)
        RX packets 163371  bytes 47862745 (47.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1280831  bytes 76196055 (76.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4156  bytes 297995 (297.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4156  bytes 297995 (297.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
```