Centro de Enseñanza Técnica Industrial

Desarrollo de Software

Documentación de nmap

Jesús Alberto Aréchiga Carrillo

22310439 5N

Profesor

José Francisco Pérez Reyes

Noviembre 2024

Guadalajara, Jalisco

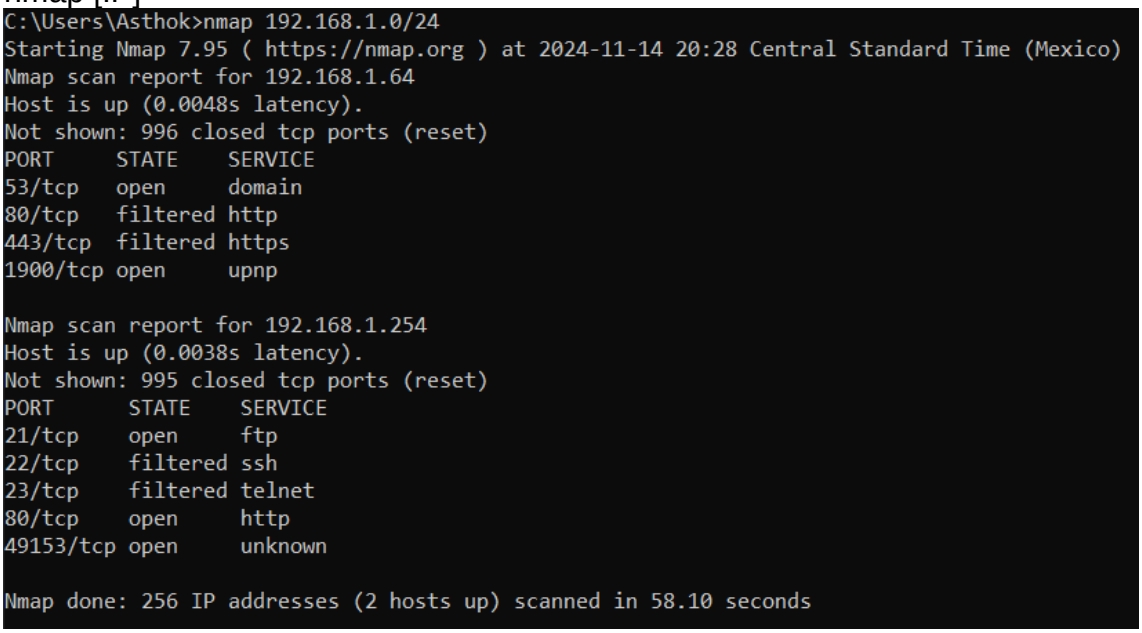
Introducción

El comando nmap (Network Mapper) es una herramienta de código abierto ampliamente utilizada en la auditoría de seguridad y el análisis de redes. Su principal función es descubrir hosts y servicios en una red, lo que permite a los administradores de sistemas y especialistas en seguridad identificar posibles puntos de vulnerabilidad y conocer la infraestructura subyacente.

Desarrollo

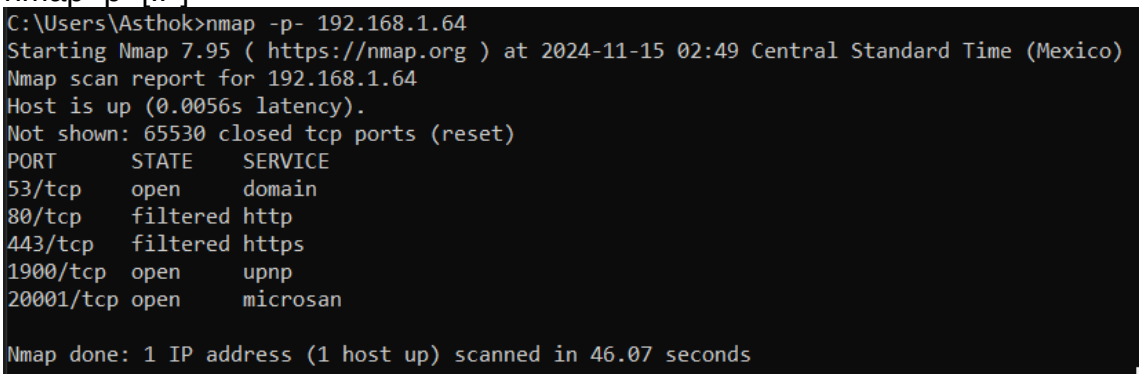
El comando nmap tiene muchas opciones para usarse, en esta práctica se van a usar 10 combinaciones de argumentos y mostrar la función que hacen dichas combinaciones.

1- nmap [IP]



Escanea una subred completa (en este caso, la red de clase C 192.168.1.0) para encontrar hosts activos.

2- nmap -p- [IP]



Escanea todos los puertos de una dirección IP en específico. Es útil para descubrir servicios que no están en los puertos comunes.

3- nmap -p [IP]

```
C:\Users\Asthok>nmap -p 80,443,20001 192.168.1.64
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-15 03:06 Central Standard Time (Mexico)
Nmap scan report for 192.168.1.64
Host is up (0.0038s latency).

PORT      STATE    SERVICE
80/tcp    filtered http
443/tcp   filtered https
20001/tcp open     microsan

Nmap done: 1 IP address (1 host up) scanned in 1.51 seconds
```

Escanea puertos específicos de una dirección IP

4- nmap -sV [IP]

```
C:\Users\Asthok>nmap -sV 192.168.1.64
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-15 03:09 Central Standard Time (Mexico)
Nmap scan report for 192.168.1.64
Host is up (0.0057s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE    SERVICE VERSION
53/tcp   open     domain  dnsmasq 2.83
80/tcp   filtered http
443/tcp  filtered https
1900/tcp open     upnp    MiniUPnP 1.8 (TP-LINK router; UPnP 1.1)
Service Info: Device: broadband router

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.88 seconds
```

Escanea dando las versiones de los servicios que se están ejecutando

5- nmap -sS [IP]

```
C:\Users\Asthok>nmap -sS 192.168.1.64
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-15 03:13 Central Standard Time (Mexico)
Nmap scan report for 192.168.1.64
Host is up (0.0079s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE    SERVICE
53/tcp   open     domain
80/tcp   filtered http
443/tcp  filtered https
1900/tcp open     upnp

Nmap done: 1 IP address (1 host up) scanned in 2.07 seconds
```

Escanea los puertos de una diercción IP en modo sigiloso (SYN scan), que es más dificil de detectar porque no el handshake TCP.

6- nmap -O [IP]

```
C:\Users\Asthok>nmap -O 192.168.1.64
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-15 03:17 Central Standard Time (Mexico)
Nmap scan report for 192.168.1.64
Host is up (0.0040s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE    SERVICE
53/tcp   open     domain
80/tcp   filtered http
443/tcp  filtered https
1900/tcp open     upnp
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3.18
OS details: Linux 3.18 (OpenWrt)
Network Distance: 1 hop
```

Escanea la dirección IP brindando información del sistema operativo que se está utilizando.

7- nmap -T4 192.168.1.64

```
C:\Users\Asthok>nmap -T4 192.168.1.64
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-15 03:19 Central Standard Time (Mexico)
Nmap scan report for 192.168.1.64
Host is up (0.0058s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE    SERVICE
53/tcp   open     domain
80/tcp   filtered http
443/tcp  filtered https
1900/tcp open     upnp

Nmap done: 1 IP address (1 host up) scanned in 1.91 seconds
```

Escanea los puertos de una dirección IP en modo rápido. Utiliza el nivel de velocidad T4, que es más rápido que el escaneo normal. Ideal para hacer un escaneo más ágil, pero consume más recursos.

8- nmap -Pn [IP]

```
C:\Users\Asthok>nmap -Pn 192.168.1.64
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-15 03:21 Central Standard Time (Mexico)
Nmap scan report for 192.168.1.64
Host is up (0.0055s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE    SERVICE
53/tcp   open     domain
80/tcp   filtered http
443/tcp  filtered https
1900/tcp open     upnp

Nmap done: 1 IP address (1 host up) scanned in 1.94 seconds
```

Escanea los puertos de una dirección IP sin ping para evitar la detección de ICMP. Útil para escanear dispositivos que bloquean solicitudes ICMP.

9- nmap -sA [IP]

```
C:\Users\Asthok>nmap -sA 192.168.1.64
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-15 03:28 Central Standard Time (Mexico)
Nmap scan report for 192.168.1.64
Host is up (0.0052s latency).
Not shown: 998 unfiltered tcp ports (reset)
PORT    STATE    SERVICE
80/tcp  filtered http
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
```

Escanea puertos de un a dirección IP con detección de firewall o presencia de sistemas de filtrado de paquetes

10- nmap –traceroute [IP]

```
C:\Users\Asthok>nmap --traceroute 192.168.1.64
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-15 03:30 Central Standard Time (Mexico)
Nmap scan report for 192.168.1.64
Host is up (0.0046s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE    SERVICE
53/tcp   open     domain
80/tcp   filtered http
443/tcp  filtered https
1900/tcp open     upnp

TRACEROUTE (using port 21/tcp)
HOP RTT     ADDRESS
1   4.00 ms 192.168.1.64

Nmap done: 1 IP address (1 host up) scanned in 2.06 seconds
```

Muestra la ruta que los paquetes siguen para llegar al objetivo, lo que ayuda a identificar los saltos de red y posibles problemas en la ruta.