

Nombre: CARLOS DAVID ESCAMILLA

Código: 202311162

Ejercicio 2: Uso Práctico de Nmap

Instalación Nmap

Instalación máquina virtual

Conocer la puerta de enlace predeterminada y la IP del equipo.

```
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\pagan>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet Ethernet 2:

    Sufijo DNS específico para la conexión. . :
    Vínculo: dirección IPv6 local. . . : fe80::9d05:7651:658f:340a%53
    Dirección IPv4. . . . . : 192.168.56.1
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :

Adaptador de LAN inalámbrica Conexión de área local* 9:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 10:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Wi-Fi:

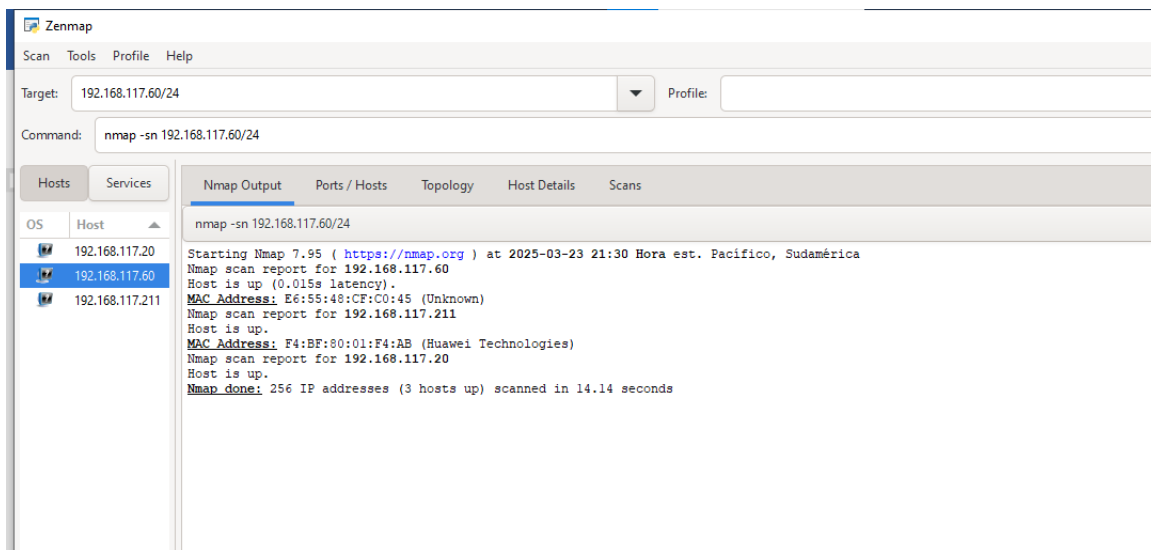
    Sufijo DNS específico para la conexión. . :
    Vínculo: dirección IPv6 local. . . : fe80::6bd3:b96f:153d:c3c8%10
    Dirección IPv4. . . . . : 192.168.117.20
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.117.60

Adaptador de Ethernet Conexión de red Bluetooth:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :
```

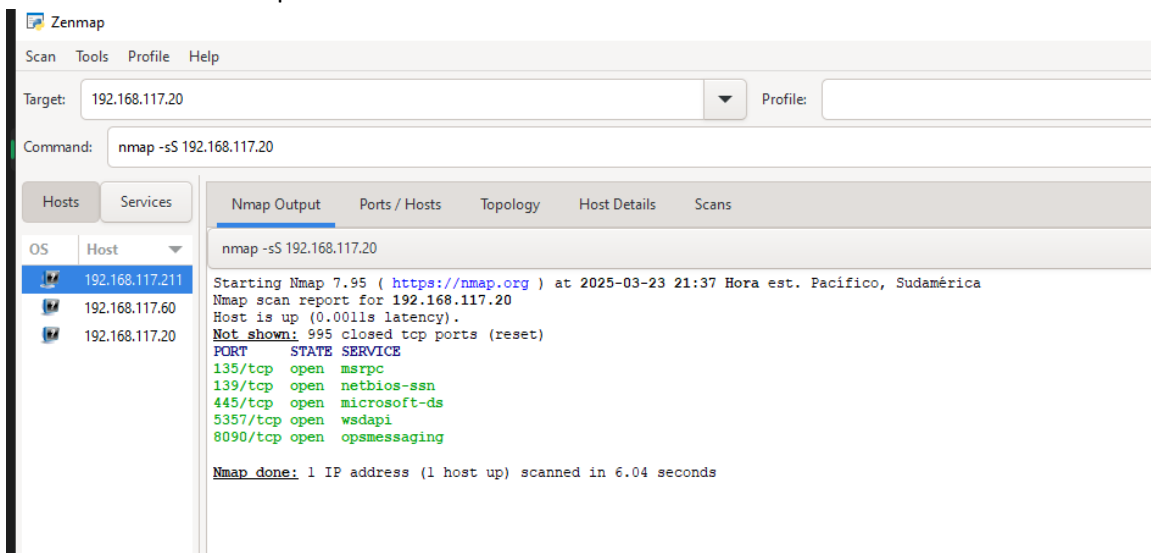
Descubriendo dispositivos en la red

- Comando: nmap -sn 192.168.117.60/24, para identificar direcciones IP y nombres de host.

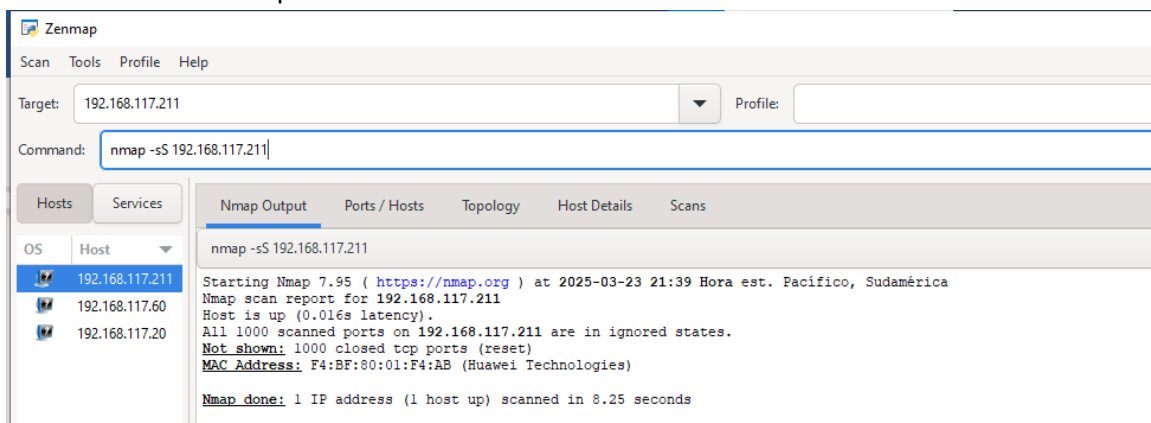


Después de hacer el escaneo se evidencia que hay tres dispositivos conectados a la red

- Comando nmap -sn 192.168.117.20



- Comando nmap -sn 192.168.117.211



- Comando nmap -sS 192.168.117.60

Zenmap

Scan Tools Profile Help

Target: 192.168.117.60 Profile:

Command: nmap -sS 192.168.117.60

Hosts Services

OS Host

192.168.117.211

192.168.117.60

192.168.117.20

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sS 192.168.117.60

Starting Nmap 7.95 (<https://nmap.org>) at 2025-03-23 21:43 Hora est. Pacífico, Sudamérica

Nmap scan report for 192.168.117.60

Host is up (0.013s latency).

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE

53/tcp open domain

MAC Address: E6:55:48:CF:C0:45 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 7.47 seconds

- Comando: nmap -sT 192.168.117.20

Zenmap

Scan Tools Profile Help

Target: 192.168.117.20 Profile:

Command: nmap -sT 192.168.117.20

Hosts Services

OS Host

192.168.117.211

192.168.117.60

192.168.117.20

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sT 192.168.117.20

Starting Nmap 7.95 (<https://nmap.org>) at 2025-03-23 21:46 Hora est. Pacífico, Sudamérica

Nmap scan report for 192.168.117.20

Host is up (0.00090s latency).

Not shown: 995 filtered tcp ports (no-response)

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

5357/tcp open wsdapi

8090/tcp open opsmessaging

Nmap done: 1 IP address (1 host up) scanned in 14.18 seconds

- Comando: nmap -sT 192.168.117.211

Zenmap

Scan Tools Profile Help

Target: 192.168.117.211 Profile:

Command: nmap -sT 192.168.117.211

Hosts Services

OS Host

192.168.117.211

192.168.117.60

192.168.117.20

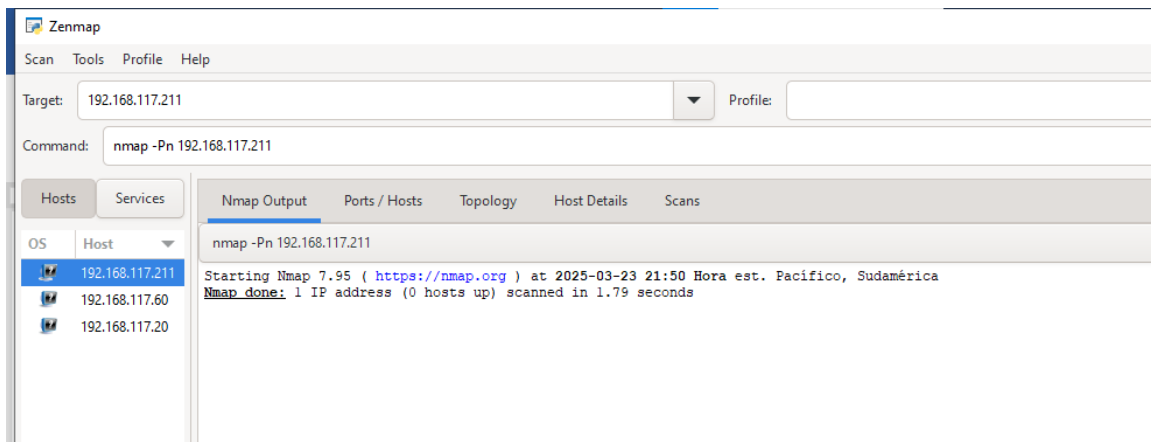
Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sT 192.168.117.211

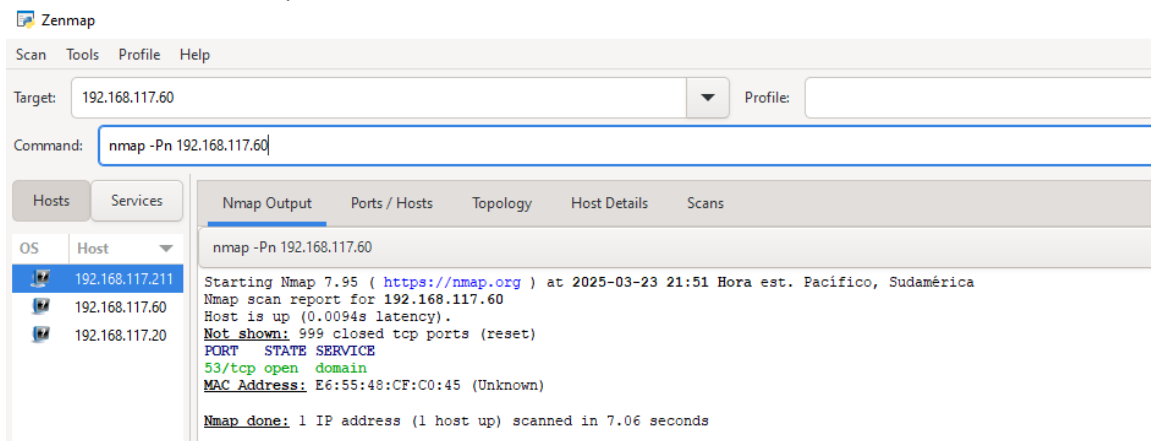
Starting Nmap 7.95 (<https://nmap.org>) at 2025-03-23 21:49 Hora est. Pacífico, Sudamérica

Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn

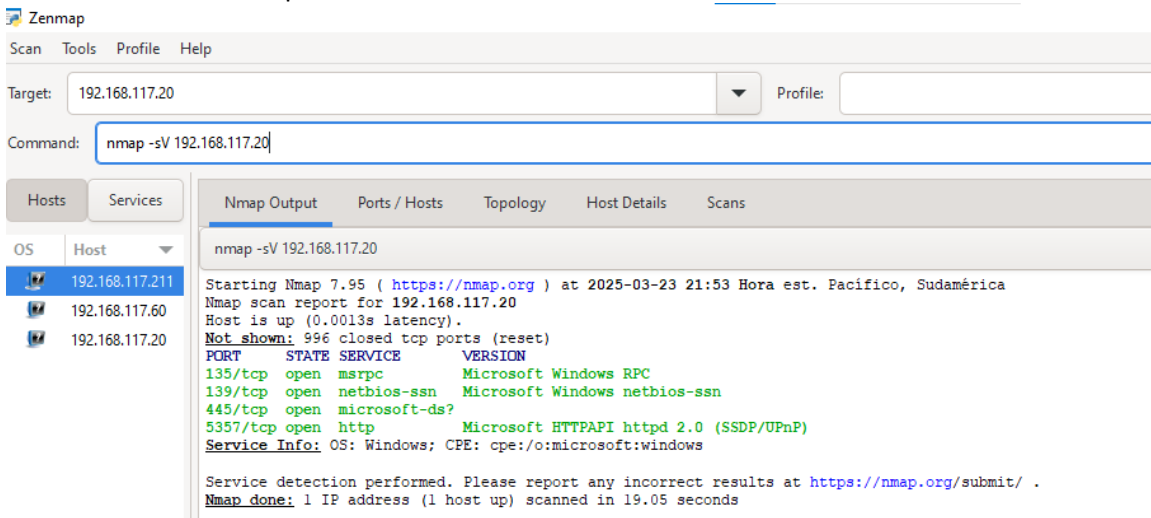
Nmap done: 1 IP address (0 hosts up) scanned in 1.78 seconds



- Comando: `nmap -sT 192.168.117.60`



- Comando: `nmap -sV 192.168.117.20`



- Comando: `nmap -sV 192.168.117.211`

Zenmap

Scan Tools Profile Help

Target: 192.168.117.211 Profile:

Command: `nmap -sV 192.168.117.211`

Hosts Services

OS Host

192.168.117.211

192.168.117.60

192.168.117.20

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sV 192.168.117.211

Starting Nmap 7.95 (<https://nmap.org>) at 2025-03-23 21:55 Hora est. Pacífico, Sudamérica
 Nmap scan report for 192.168.117.211
 Host is up (0.016s latency).
 All 1000 scanned ports on 192.168.117.211 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: F4:BF:80:01:F4:AB (Huawei Technologies)

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 9.21 seconds

- Comando: `nmap -sV 192.168.117.60`

Zenmap

Scan Tools Profile Help

Target: 192.168.117.60 Profile:

Command: `nmap -sV 192.168.117.60`

Hosts Services

OS Host

192.168.117.211

192.168.117.60

192.168.117.20

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sV 192.168.117.60

Starting Nmap 7.95 (<https://nmap.org>) at 2025-03-23 21:56 Hora est. Pacífico, Sudamérica
 Nmap scan report for 192.168.117.60
 Host is up (0.0088s latency).
Not shown: 999 closed tcp ports (reset)
 PORT STATE SERVICE VERSION
 53/tcp open domain dnsmasq 2.51
MAC Address: E6:55:48:CF:C0:45 (Unknown)

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 13.51 seconds

- Comando: `nmap -O 192.168.117.20`

Zenmap

Scan Tools Profile Help

Target: 192.168.117.20 Profile:

Command: `nmap -O 192.168.117.20`

Hosts Services

OS Host

192.168.117.211

192.168.117.60

192.168.117.20

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -O 192.168.117.20

Starting Nmap 7.95 (<https://nmap.org>) at 2025-03-23 21:59 Hora est. Pacífico, Sudamérica
 Nmap scan report for 192.168.117.20
 Host is up (0.00049s latency).
Not shown: 996 closed tcp ports (reset)
 PORT STATE SERVICE
 135/tcp open msrpc
 139/tcp open netbios-ssn
 445/tcp open microsoft-ds
 5357/tcp open wsdapi
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 21H2
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 7.06 seconds

- Comando: `nmap -O 192.168.117.211`

The screenshot shows the Zenmap application window. The 'Target' field is set to '192.168.117.211'. The 'Command' field contains 'sudo -O 192.168.117.211'. The 'Hosts' tab is selected, showing a list of hosts: 192.168.117.211 (selected), 192.168.117.60, and 192.168.117.20. The 'Nmap Output' tab is active, displaying the following text:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-23 22:02 Hora est. Pacifico, Sudamérica
Nmap scan report for 192.168.117.211
Host is up (0.032s latency).
All 1000 scanned ports on 192.168.117.211 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: F4:BF:80:01:F4:AB (Huawei Technologies)
Too many fingerprints match this host to give specific OS details
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 9.60 seconds
```

- Comando: `nmap -O 192.168.117.60`

The screenshot shows the Zenmap application window. The 'Target' field is set to '192.168.117.60'. The 'Command' field contains 'nmap -O 192.168.117.60'. The 'Hosts' tab is selected, showing a list of hosts: 192.168.117.211, 192.168.117.60 (selected), and 192.168.117.20. The 'Nmap Output' tab is active, displaying the following text:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-23 22:04 Hora est. Pacifico, Sudamérica
Nmap scan report for 192.168.117.60
Host is up (0.0071s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: E6:55:48:CF:C0:45 (Unknown)
Aggressive OS guesses: Android 9 (Linux 4.9) (96%), Android 10 (Linux 4.14) (94%), Android 9 - 10 (Linux 4.9 - 4.14) (93%), OpenWrt 22.03 (Linux 5.10) (93%), Linux 2.6.32 - 3.10 (93%), Asus RT-N10 router or AXIS 211A Network Camera (Linux 2.6) (91%), Linux 2.6.18 (91%), Linux 2.6.18 - 2.6.32 (90%), Aruba ArubaOS-CX 10.04 (90%), Linux 2.6.16 (90%)
No exact OS matches for host (test conditions non-ideal).
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 10.94 seconds
```