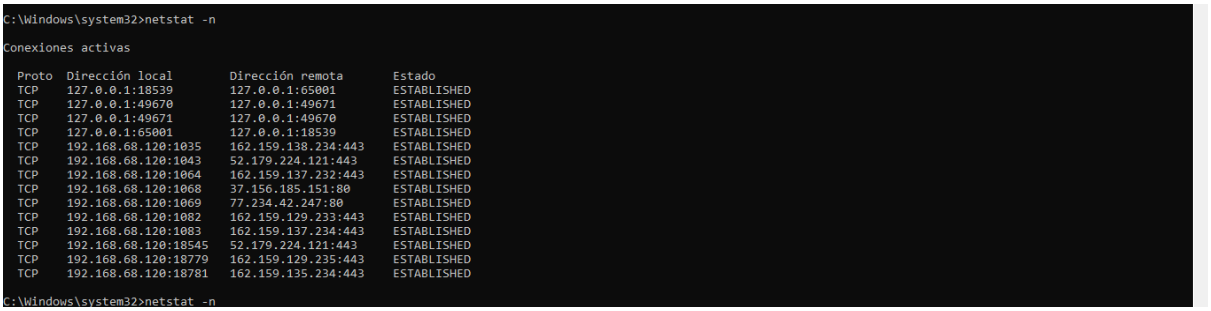
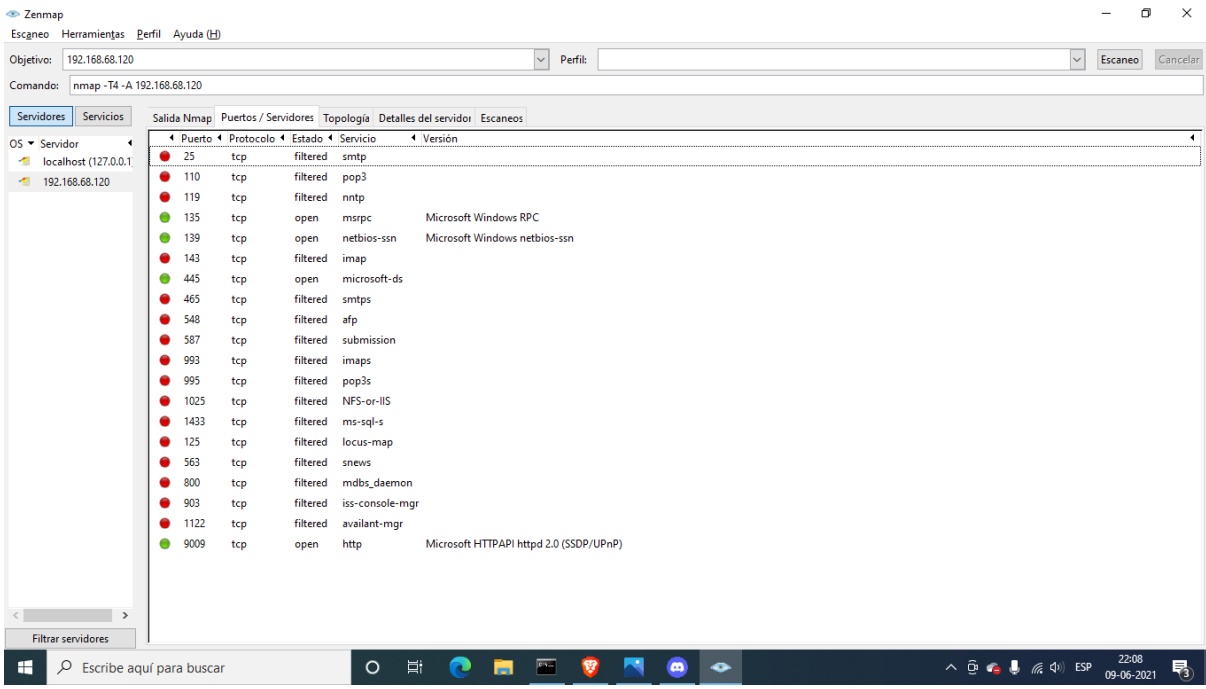
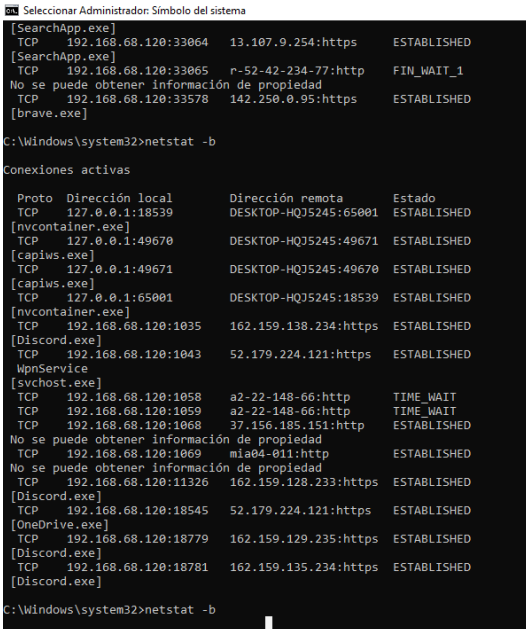
1. Identificar todas las conexiones y puertos de escucha de su máquina con las direcciones y los números de puerto en forma numérica. Esto se hace utilizando la herramienta netstat, usando la bandera -n.



```
C:\Windows\system32>netstat -n

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    127.0.0.1:18539        127.0.0.1:65001        ESTABLISHED
  TCP    127.0.0.1:49670        127.0.0.1:49671        ESTABLISHED
  TCP    127.0.0.1:49671        127.0.0.1:49670        ESTABLISHED
  TCP    127.0.0.1:65001        127.0.0.1:18539        ESTABLISHED
  TCP    192.168.68.120:1035    162.159.138.234:443    ESTABLISHED
  TCP    192.168.68.120:1043    52.179.224.121:443     ESTABLISHED
  TCP    192.168.68.120:1064    162.159.137.232:443    ESTABLISHED
  TCP    192.168.68.120:1068    37.156.185.151:80      ESTABLISHED
  TCP    192.168.68.120:1069    77.234.42.247:80       ESTABLISHED
  TCP    192.168.68.120:1082    162.159.129.233:443    ESTABLISHED
  TCP    192.168.68.120:1083    162.159.137.234:443    ESTABLISHED
  TCP    192.168.68.120:18545   52.179.224.121:443     ESTABLISHED
  TCP    192.168.68.120:18779   162.159.129.235:443    ESTABLISHED
  TCP    192.168.68.120:18781   162.159.135.234:443    ESTABLISHED

C:\Windows\system32>netstat -n
```



2. Identificar en su máquina los procesos vinculados a los puertos identificados y cierre aquellos procesos que no son imprescindibles para el desarrollo del presente laboratorio. Para ver los servicios que utilizan los puertos se usan netstat con la bandera -b.



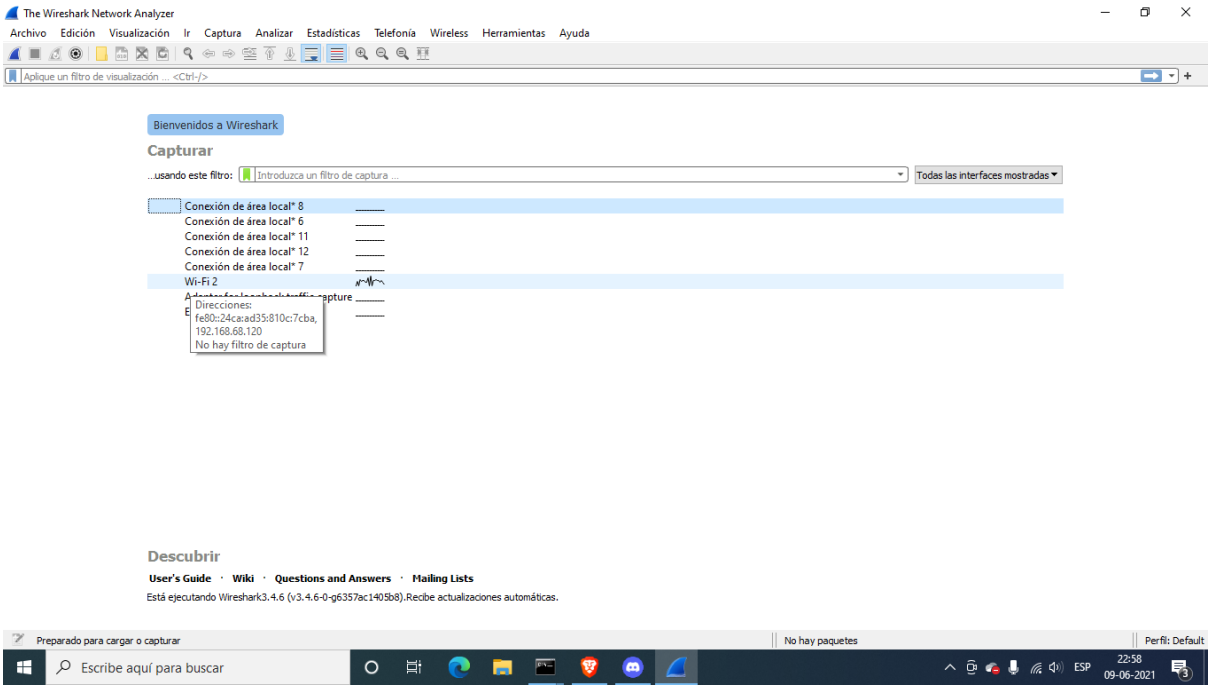
Puerto 135:El "Administrador de control de servicios DCOM (modelo de objetos componentes distribuidos)" de Microsoft que se ejecuta en la computadora del usuario utiliza el puerto 135. El puerto 135 expone dónde se pueden encontrar los servicios DCOM en una máquina. Las herramientas de piratas informáticos como "epdump" (Endpoint Dump) pueden identificar inmediatamente todos los servidores / servicios relacionados con DCOM que se ejecutan en el equipo de alojamiento del usuario y compararlos con exploits conocidos contra esos servicios. Por lo tanto, el puerto 135 no debe estar expuesto a Internet y debe bloquearse.

Puerto 139: Es un dispositivo de programación en red, es uno de los más odiados por los administradores de red, ya que hace que la red sea vulnerable a ataques de los piratas informáticos. El puerto 139 es utilizado por servicio de sesión NetBEUI, que imita al TCP estableciendo una sesión con la computadora remota. Una vez que una sesión ha sido establecida, muchos mensajes pueden pasar idas y vuelta en la red.

Puerto 445:
Puerto 9009: Es utilizado por el protocolo de control de transmisión, este puerto garantiza la entrega de paquetes de datos en el mismo orden en que fueron enviados.

svchost.exe → gestor de servicios de Windows.
capiws.exe → proceso de OpenVPN Connect.
nvcontainer.exe → proceso asociado a la tarjeta de video.

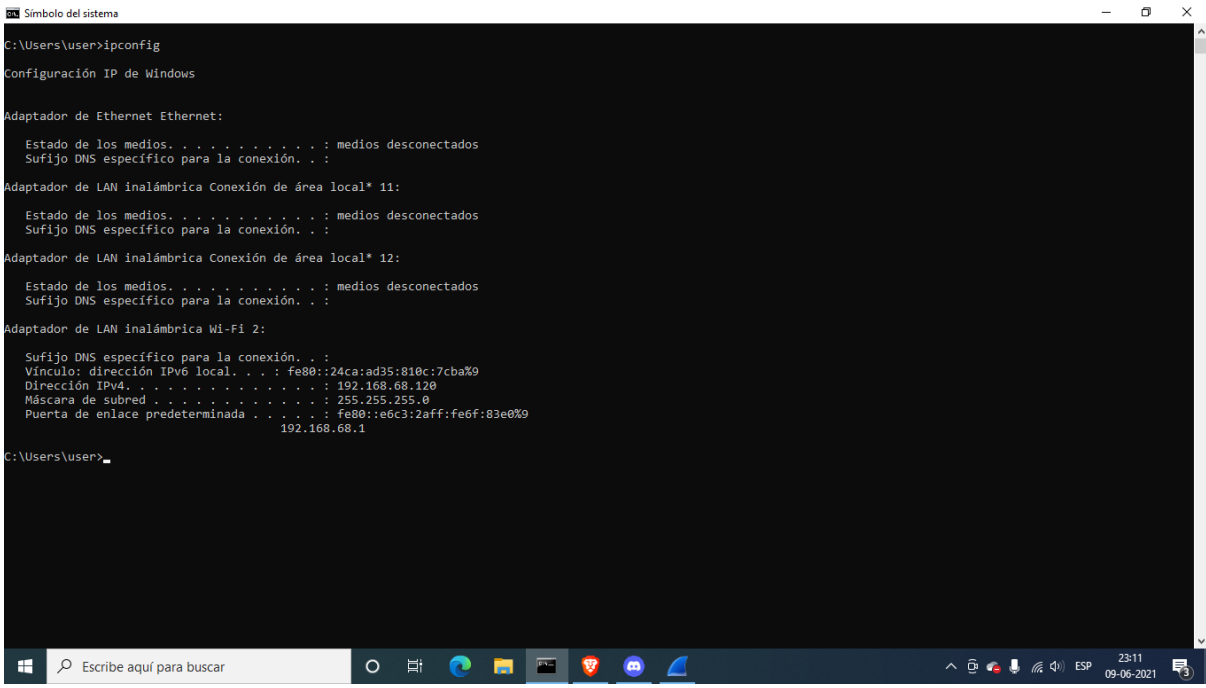
3. Encender wireshark y



comenzar a escuchar el tráfico de la red.

4. Identificar cuál es su IP.

   La IP que sale en la columna Source es 192.168.68.120, que coincide con el resultado entregado ejecutando el comando ipconfig.



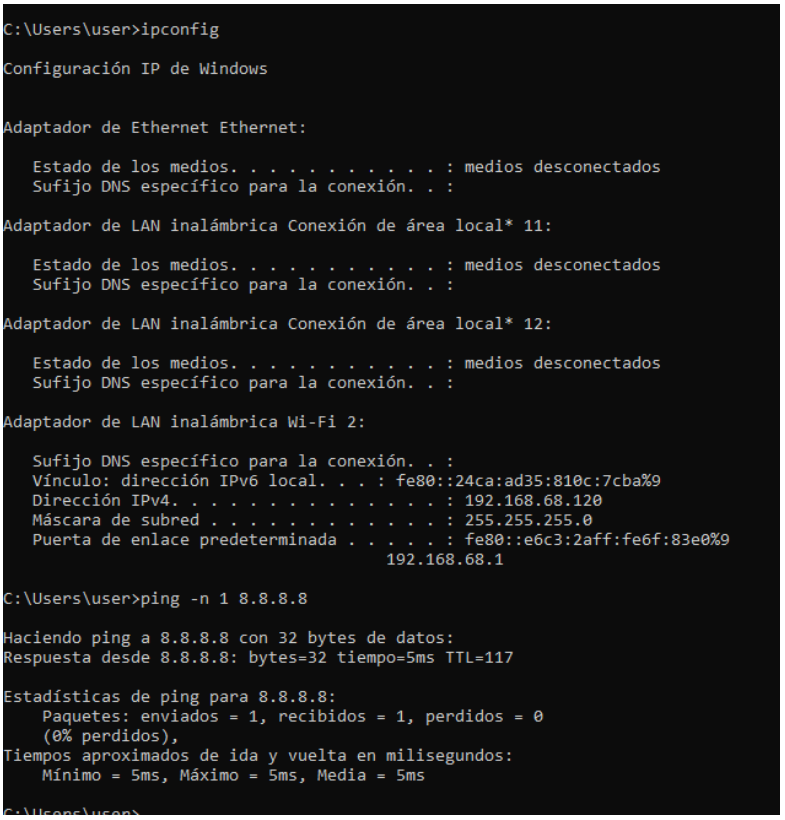
5. Utilizar un solo paquete ICMP tipo 8 (Request) para comprobar la conectividad a través de una respuesta tipo 0 (Eco) con la dirección IP 8.8.8.8.

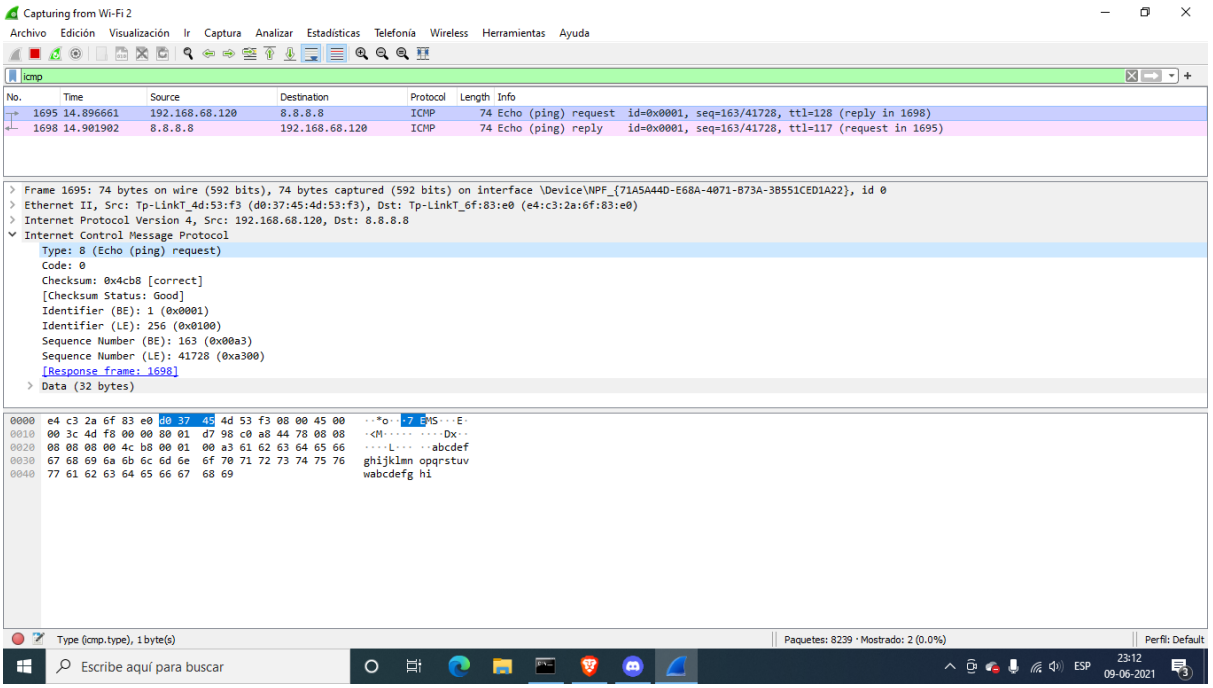
   - Para intercambiar datos de estado o mensajes de error, los nodos recurren al Internet Control Message Protocol (ICMP) en las redes TCP/IP. Concretamente, los servidores de aplicaciones y las puertas de acceso como

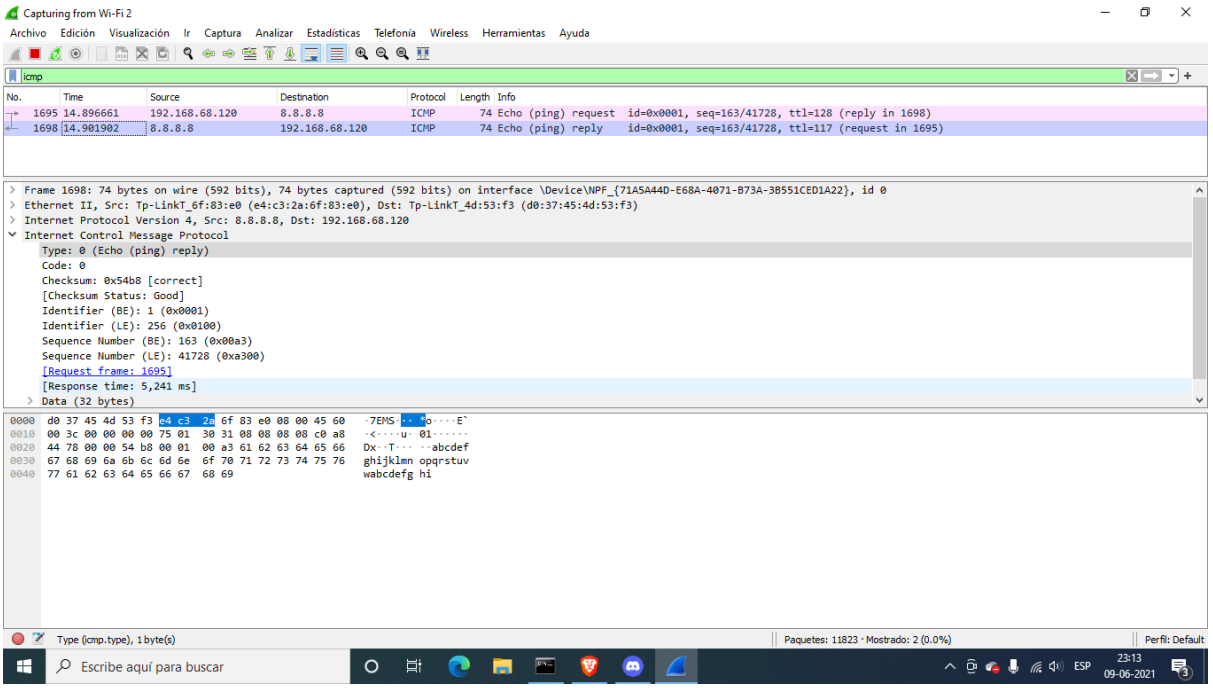
los routers, utilizan esta implementación del protocolo IP para devolver mensajes sobre problemas con datagramas al remitente del paquete.

- ICMP tipo 8 corresponde a un Ping de red.
- Esta simple pero útil herramienta de diagnóstico es la solución más sencilla para comprobar la accesibilidad de un determinado host en la red. Para ello, el ping envía, por un lado, un paquete IP incluida una “Echo Request” ICMP(6) (tipo 8 o 128), al que, tras su recepción, el receptor responderá con un paquete de datos que contiene la entrada ICMP “Echo Reply” (tipo 0 o 129). Si no se localiza al sistema al que se ha enviado el ping, la última estación de red disponible enviará un paquete de respuesta, el cual se amplía con un componente ICMP, es decir, tipo 3 o 1 “Destination Unreachable” (“objetivo inalcanzable”).

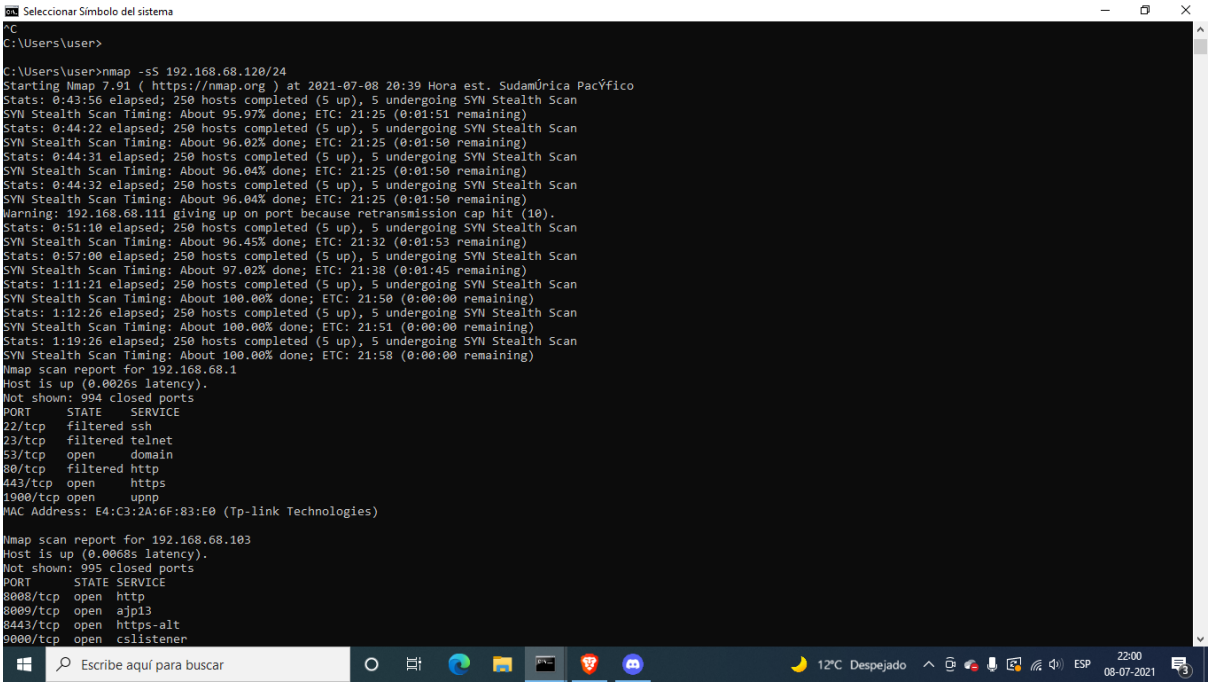
Envío de un solo paquete ICMP tipo 8 a la dirección IP 8.8.8.8

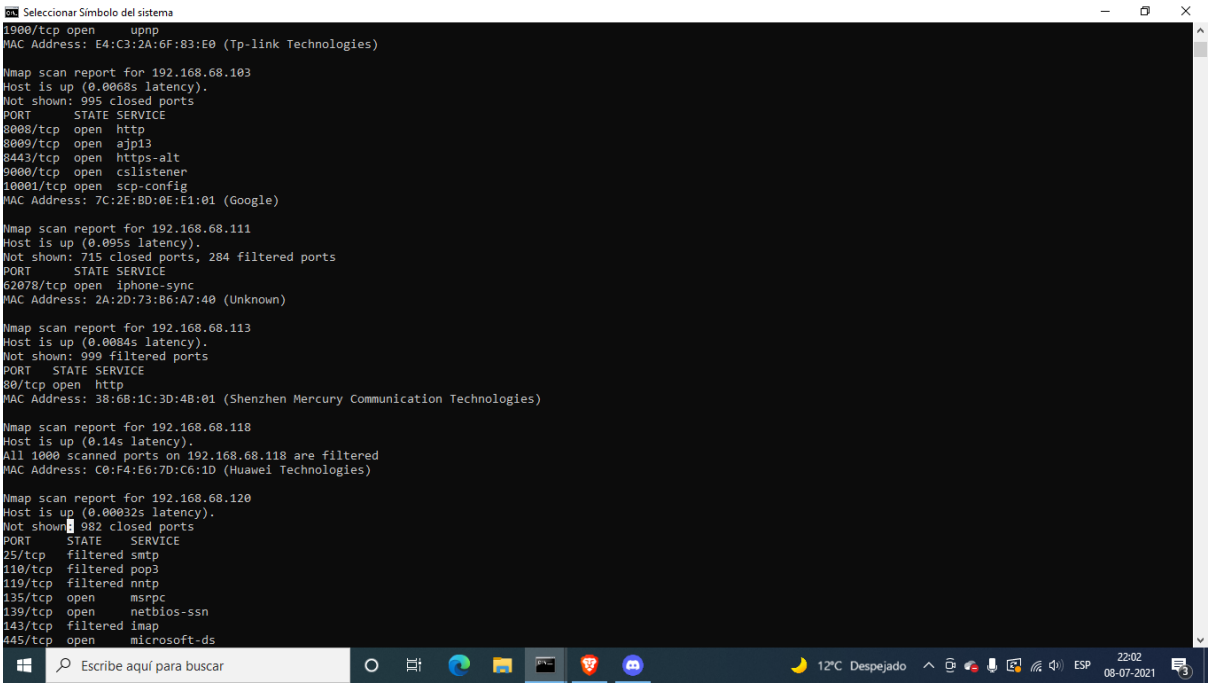


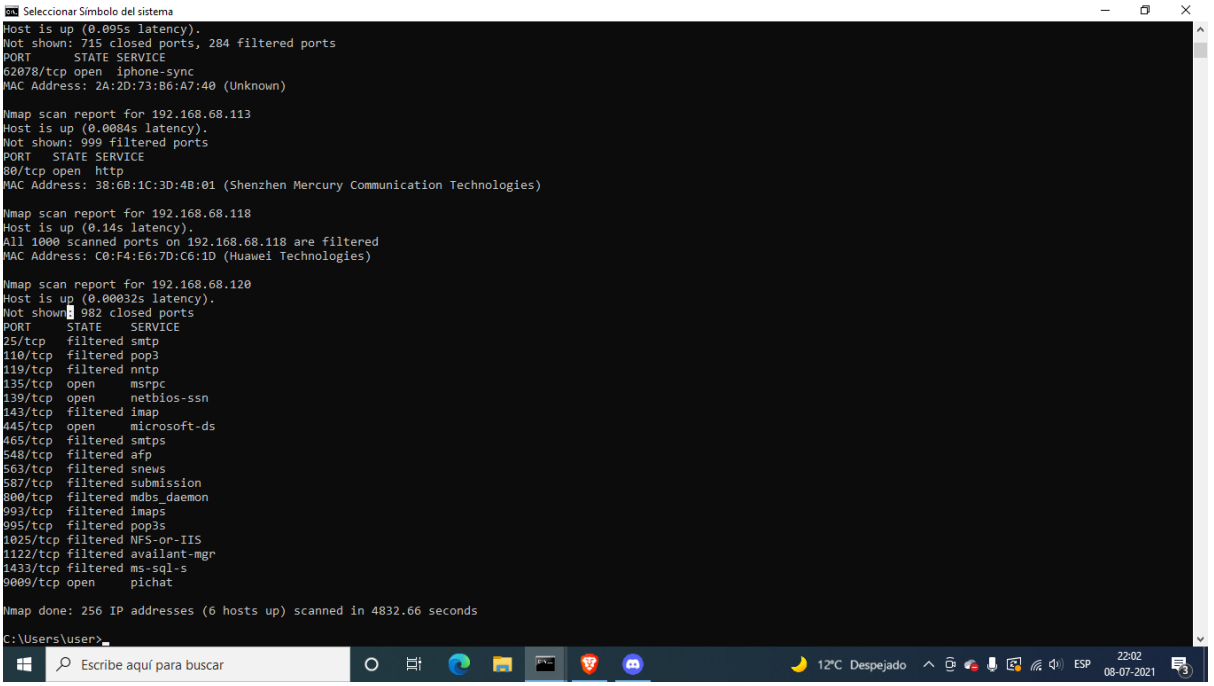




6. Escanee el rango de IP de su casa (sea sigiloso).
   Preguntar al ayudante - profesor
   Debido al servicio contratado de internet, la máscara de red es 255.255.255.0, teniendo un rango de 24.
   nmap [ip]/24

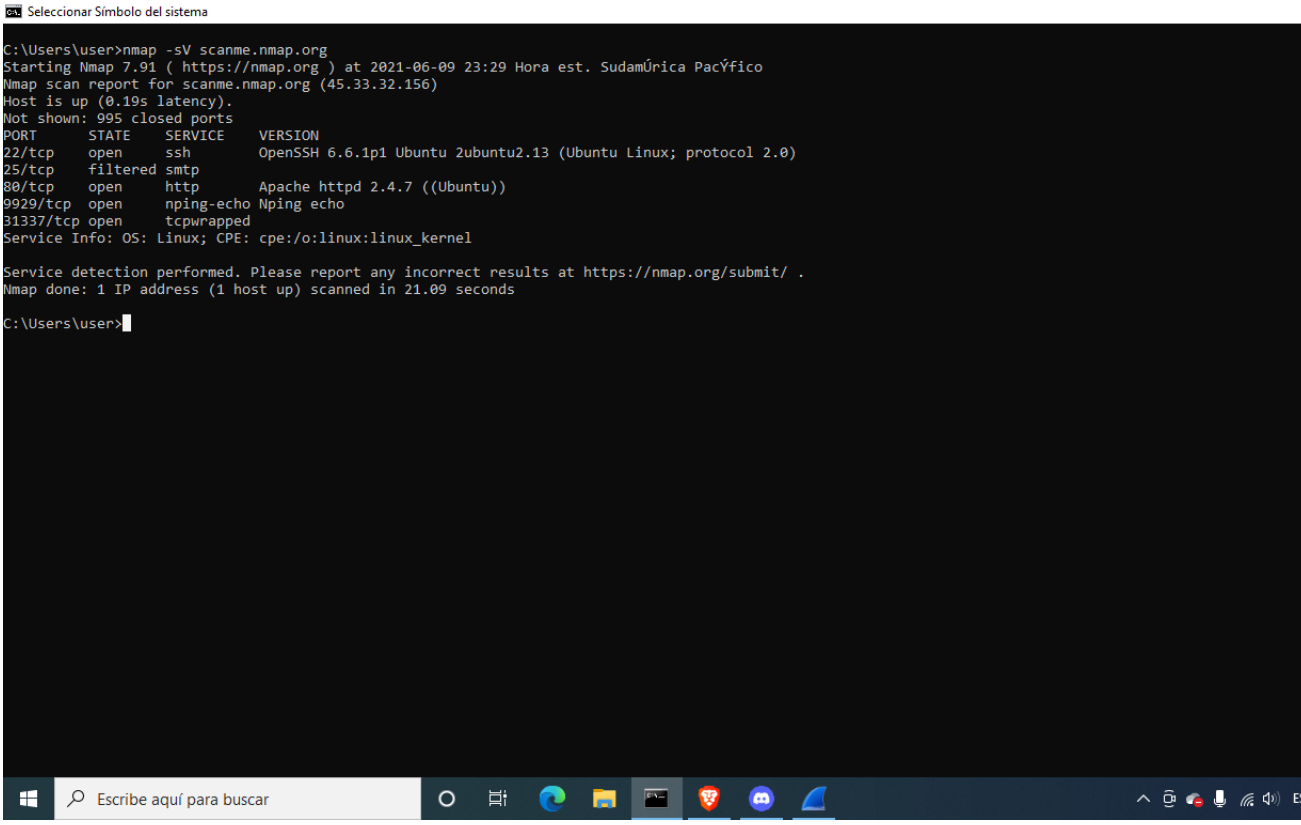

Seleccionar Símbolo del sistema
^C
C:\Users\user>
C:\Users\user>nmap -sS 192.168.68.120/24
Starting Nmap 7.91 (https://nmap.org) at 2021-07-08 20:39 Hora est. SudamÚrica PacÝfico
Stats: 0:43:56 elapsed; 250 hosts completed (5 up), 5 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 95.97% done; ETC: 21:25 (0:01:51 remaining)
Stats: 0:44:22 elapsed; 250 hosts completed (5 up), 5 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.02% done; ETC: 21:25 (0:01:50 remaining)
Stats: 0:44:31 elapsed; 250 hosts completed (5 up), 5 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.04% done; ETC: 21:25 (0:01:50 remaining)
Stats: 0:44:32 elapsed; 250 hosts completed (5 up), 5 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.04% done; ETC: 21:25 (0:01:50 remaining)
Warning: 192.168.68.111 giving up on port because retransmission cap hit (10).
Stats: 0:51:10 elapsed; 250 hosts completed (5 up), 5 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.45% done; ETC: 21:32 (0:01:53 remaining)
Stats: 0:57:00 elapsed; 250 hosts completed (5 up), 5 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 97.02% done; ETC: 21:38 (0:01:45 remaining)
Stats: 1:11:21 elapsed; 250 hosts completed (5 up), 5 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 100.00% done; ETC: 21:50 (0:00:00 remaining)
Stats: 1:12:26 elapsed; 250 hosts completed (5 up), 5 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 100.00% done; ETC: 21:51 (0:00:00 remaining)
Stats: 1:19:26 elapsed; 250 hosts completed (5 up), 5 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 100.00% done; ETC: 21:58 (0:00:00 remaining)
Nmap scan report for 192.168.68.1
Host is up (0.0026s latency).
Not shown: 994 closed ports
PORT STATE SERVICE
22/tcp filtered ssh
23/tcp filtered telnet
53/tcp open domain
80/tcp filtered http
443/tcp open https
1900/tcp open upnp
MAC Address: E4:C3:2A:6F:83:E0 (Tp-link Technologies)
Nmap scan report for 192.168.68.103
Host is up (0.0068s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
8008/tcp open http
8009/tcp open ajp13
8443/tcp open https-alt
9000/tcp open cslistener
Escribe aquí para buscar
12°C Despejado
ESP
22:00
08-07-2021


Seleccionar Símbolo del sistema
1900/tcp open upnp
MAC Address: E4:C3:2A:6F:83:E0 (Tp-link Technologies)
Nmap scan report for 192.168.68.103
Host is up (0.0068s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
8008/tcp open http
8009/tcp open ajp13
8443/tcp open https-alt
9000/tcp open cslistener
10001/tcp open scp-config
MAC Address: 7C:2E:BD:0E:E1:01 (Google)
Nmap scan report for 192.168.68.111
Host is up (0.095s latency).
Not shown: 715 closed ports, 284 filtered ports
PORT STATE SERVICE
62078/tcp open iphone-sync
MAC Address: 2A:2D:73:B6:A7:40 (Unknown)
Nmap scan report for 192.168.68.113
Host is up (0.0084s latency).
Not shown: 999 filtered ports
PORT STATE SERVICE
80/tcp open http
MAC Address: 38:6B:1C:3D:4B:01 (Shenzhen Mercury Communication Technologies)
Nmap scan report for 192.168.68.118
Host is up (0.14s latency).
All 1000 scanned ports on 192.168.68.118 are filtered
MAC Address: C0:F4:E6:7D:C6:1D (Huawei Technologies)
Nmap scan report for 192.168.68.120
Host is up (0.00032s latency).
Not shown: 982 closed ports
PORT STATE SERVICE
25/tcp filtered smtp
110/tcp filtered pop3
119/tcp filtered nntp
135/tcp open msrpc
139/tcp open netbios-ssn
143/tcp filtered imap
445/tcp open microsoft-ds
Escribe aquí para buscar
12°C Despejado
ESP
22:02
08-07-2021



El rango IP es 192.168.68.0 - 192.168.68.255, permitiendo 256 host
Según el escáner realizado con nmap, se encontraron 6 host en la red escaneada.

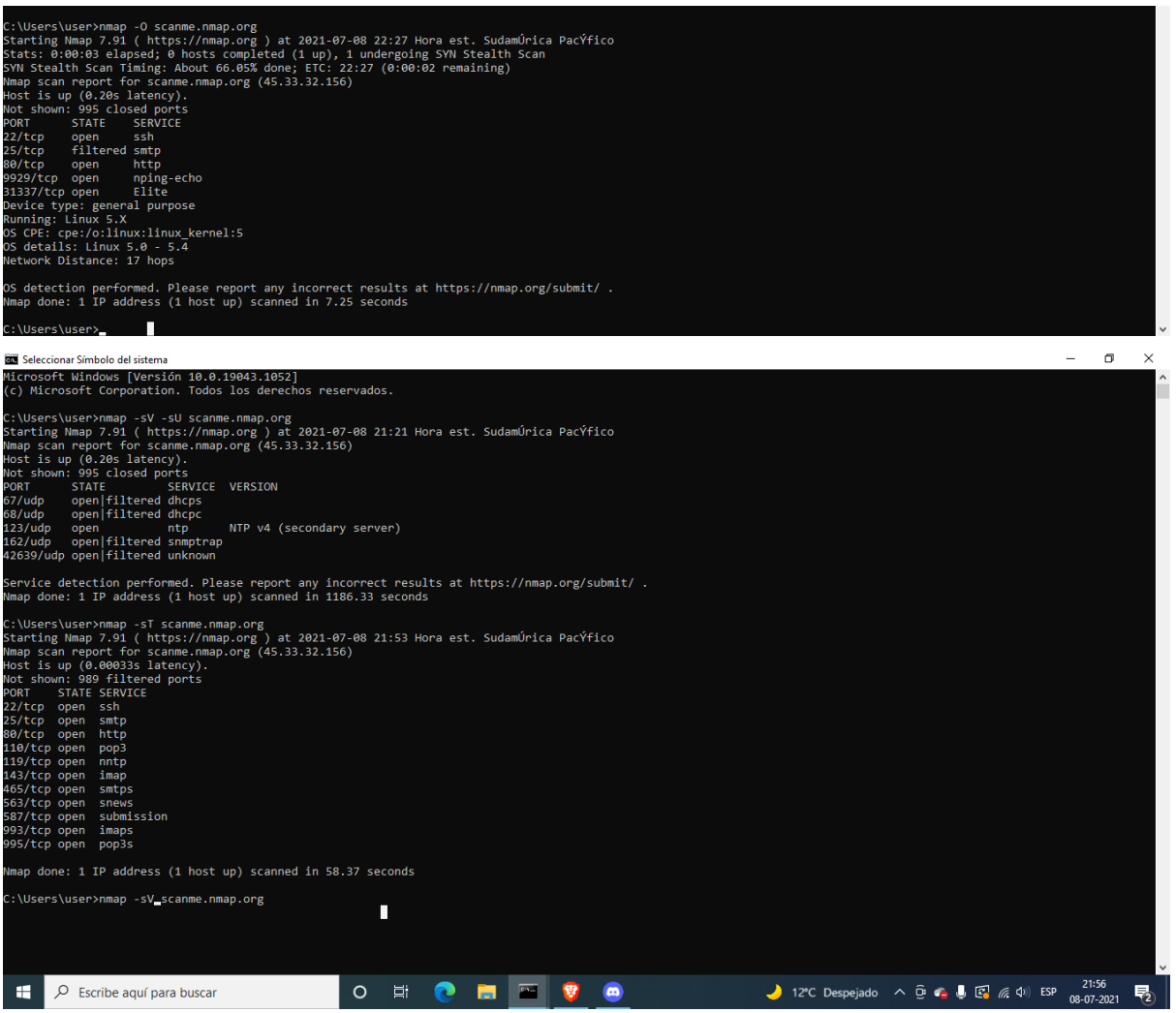
7. Escanee el objetivo e identifique (recordar mezclar opciones):
   nmap -sV -sU scanme.nmap.org
   - i. Puertos TCP y UDP utilizados
   - ii. Estado de los puertos (abiertos o filtrados)
   - iii. Sistema operativo utilizado
   - iv. Versiones de los servicios (investigue)



UDP + versiones

TCP + versiones

OS



8. Investigue vulnerabilidades sobre las versiones de los servicios encontrados . Profundice en una de las vulnerabilidades encontradas.

La función auth_password en auth-passwd.c en sshd en OpenSSH antes de 7.3 no limita la longitud de las contraseñas para la autenticación de contraseñas, lo que permite a los atacantes remotos provocar una denegación de servicio (consumo de CPU de cripta) a través de una cadena larga.

Profundizando en las vulnerabilidades que se podrían presentar por la versión de Apache que se está utilizando (2.4.7) existen los siguientes:

- La primera vulnerabilidad se identifica como CVE-2019-0221. En un servidor Apache HTTP con MPM (Módulos de MultiProcesamiento) event, worker o prefork, el código que se ejecuta en procesos o subprocesos secundarios con pocos privilegios (incluyendo scripts ejecutado por un intérprete de scripts), podría permitir a un atacante ejecutar código arbitrario con los privilegios de root manipulando el marcador.

- La segunda se identifica como CVE-2019-0217 y se da ante una condición de secuencia en mod_auth_digest cuando se está ejecutando en un servidor de

subprocesos, que podría permitir a un usuario con credenciales válidas autenticarse usando otro nombre de usuario y omitiendo las restricciones de control de acceso.

- La última vulnerabilidad grave es denominada CVE-2019-0215. Un error en mod_ssl al utilizar la verificación de certificados de cliente por ubicación con TLSv1.3, podría permitir a un atacante que soporte la autenticación Post-Handshake eludir las restricciones de control de acceso.

9. Realice un escaneo Full connect sobre uno de los servicios TCP e identifique el handshake TCP de 3 vías realizado con wireshark.
   nmap -sT scanme.nmap.org

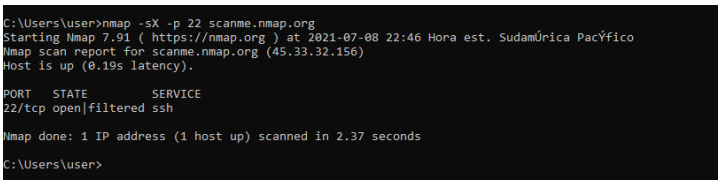
10. Realice un escaneo XMAS sobre uno de los servicios TCP e identifique el segmento con los flags activados con wireshark.

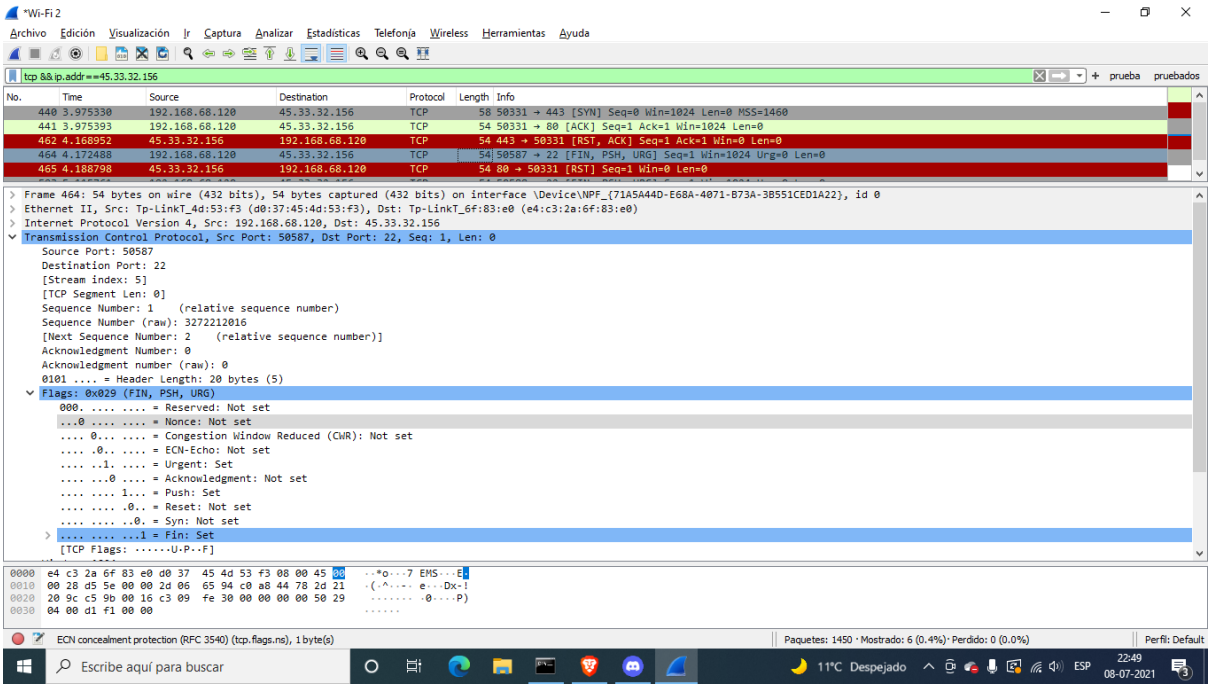
Esta técnica consiste en enviar un segmento TCP al puerto deseado del dispositivo a investigar con los bits FIN, URG y PUSH activos. Esto hace que el byte de flags contenga "00101001".
Cuando la víctima del escáner recibe este segmento, según dictan las directrices marcadas por el protocolo,

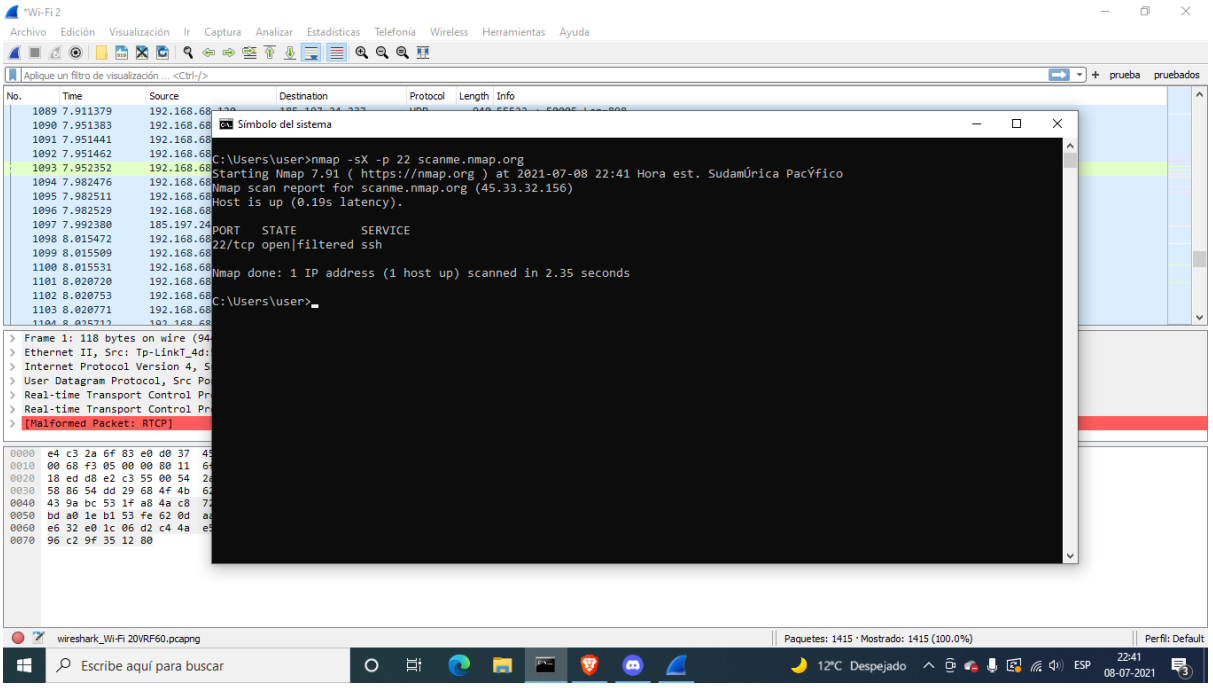
- si el puerto está cerrado, devuelve un segmento con el bit RST activo, indicando que se resetee la conexión en cliente.
- si el puerto está abierto, ignora el paquete recibido y no responde nada.

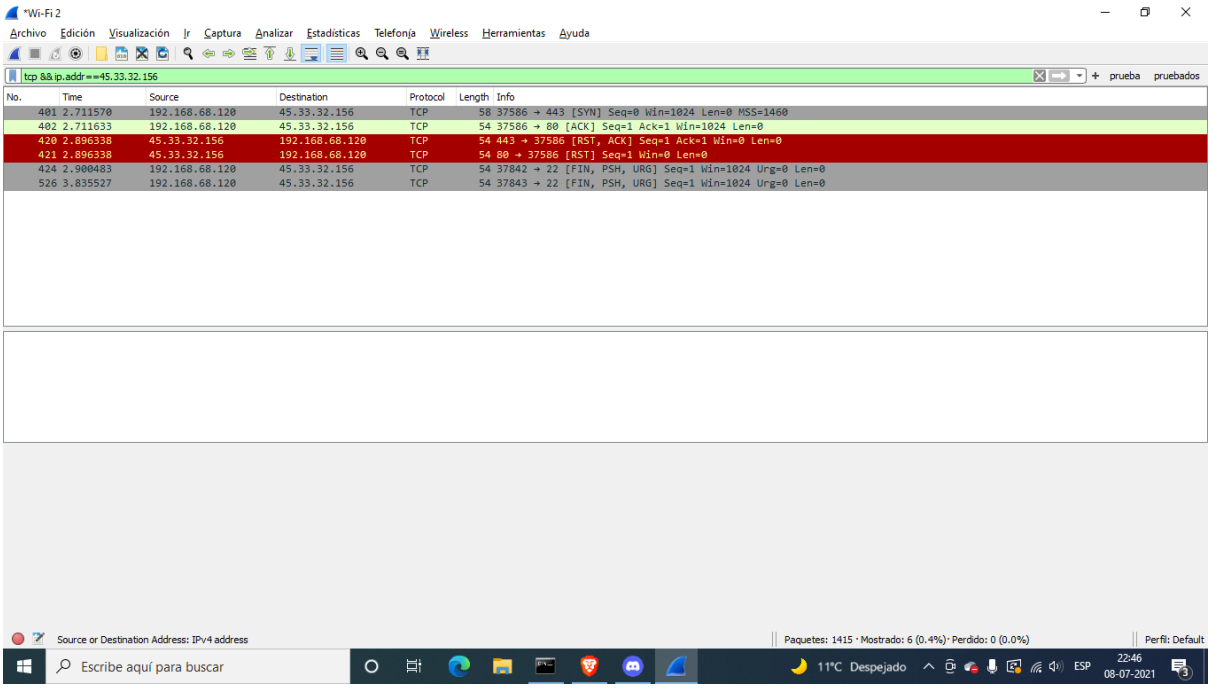
Atendiendo a la respuesta (o ausencia de ella), el atacante puede determinar el estado del puerto que está investigando de una forma realmente silenciosa, puesto que no inicia ninguna conexión (como los sondeos SYN, que inician un 3-way-handshake), y sorteando a veces filtros que no esperan este tipo de combinaciones en los flags.

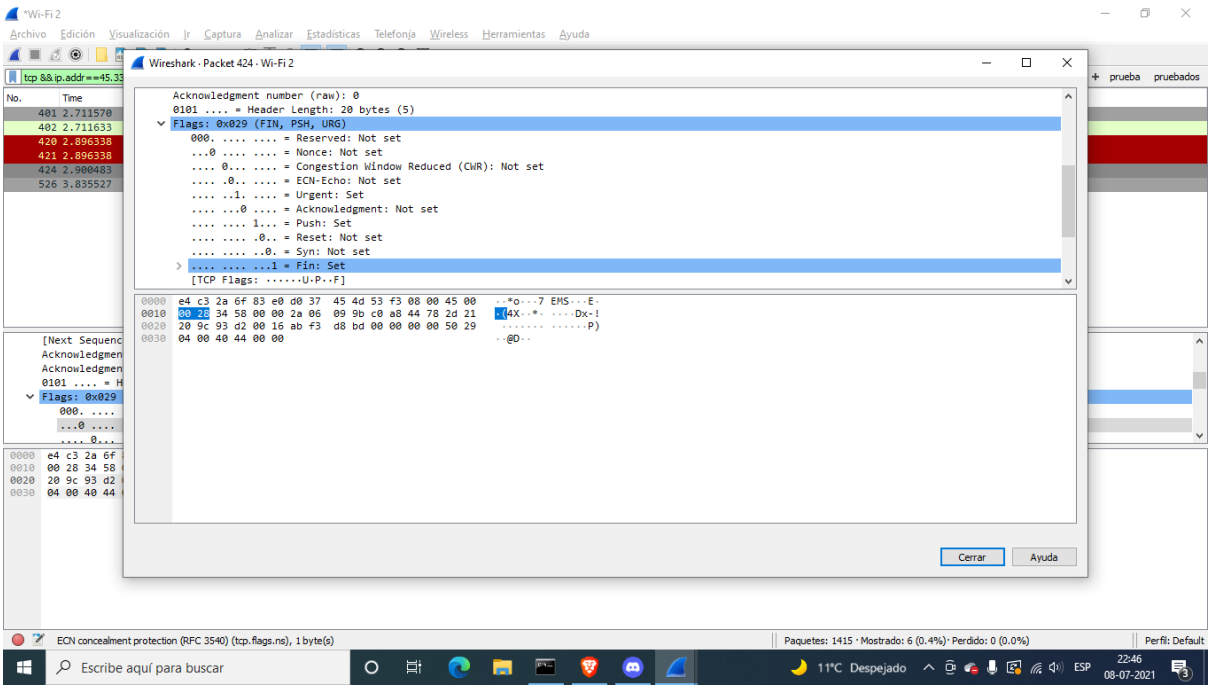
```
nmap -sX w.x.y.z
```




*Wi-Fi 2
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
tcp && ip.addr==45.33.32.156
prueba pruebados
No. Time Source Destination Protocol Length Info
440 3.975330 192.168.68.120 45.33.32.156 TCP 58 50331 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
441 3.975393 192.168.68.120 45.33.32.156 TCP 54 50331 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
462 4.168952 45.33.32.156 192.168.68.120 TCP 54 443 → 50331 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
464 4.172488 192.168.68.120 45.33.32.156 TCP 54 50587 → 22 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
465 4.188798 45.33.32.156 192.168.68.120 TCP 54 80 → 50331 [RST] Seq=1 Win=0 Len=0
Frame 464: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{71A5A44D-E68A-4071-B73A-3B551CED1A22}, id 0
Ethernet II, Src: Tp-LinkT_4d:53:f3 (d0:37:45:4d:53:f3), Dst: Tp-LinkT_6f:83:e0 (e4:c3:2a:6f:83:e0)
Internet Protocol Version 4, Src: 192.168.68.120, Dst: 45.33.32.156
Transmission Control Protocol, Src Port: 50587, Dst Port: 22, Seq: 1, Len: 0
Source Port: 50587
Destination Port: 22
[Stream index: 5]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3272212016
[Next Sequence Number: 2 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0101 .... = Header Length: 20 bytes (5)
Flags: 0x029 (FIN, PSH, URG)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..1. .... = Urgent: Set
....0 .... = Acknowledgment: Not set
.... 1... = Push: Set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....1 = Fin: Set
[TCP Flags: ·····U·P··F]
0000 e4 c3 2a 6f 83 e0 d0 37 45 4d 53 f3 08 00 45 00
0010 00 28 d5 5e 00 00 2d 06 65 94 c0 a8 44 78 2d 21
0020 20 9c c5 9b 00 16 c3 09 fe 30 00 00 00 00 50 29
0030 04 00 d1 f1 00 00
ECN concealment protection (RFC 3540) (tcp.flags.ns), 1 byte(s)
Paquetes: 1450 · Mostrado: 6 (0.4%) · Perdido: 0 (0.0%)
Perfil: Default
Escribe aquí para buscar
11°C Despejado
ESP
22:49
08-07-2021


*Wi-Fi 2
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
Aplique un filtro de visualización ... <Ctrl-/>
prueba pruebados
No. Time Source Destination Protocol Length Info
1089 7.911379
1090 7.951383
1091 7.951441
1092 7.951462
1093 7.952352
1094 7.982476
1095 7.982511
1096 7.982529
1097 7.992380
1098 8.015472
1099 8.015509
1100 8.015531
1101 8.020720
1102 8.020753
1103 8.020771
Símbolo del sistema
C:\Users\user>nmap -sX -p 22 scanme.nmap.org
Starting Nmap 7.91 (https://nmap.org) at 2021-07-08 22:41 Hora est. SudamÚrica PacÝfico
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.19s latency).
PORT STATE SERVICE
22/tcp open|filtered ssh
Nmap done: 1 IP address (1 host up) scanned in 2.35 seconds
C:\Users\user>
Frame 1: 118 bytes on wire (94
Ethernet II, Src: Tp-LinkT_4d:
Internet Protocol Version 4, S
User Datagram Protocol, Src Po
Real-time Transport Control Pr
Real-time Transport Control Pr
[Malformed Packet: RTCP]
0000 e4 c3 2a 6f 83 e0 d0 37
0010 00 68 f3 05 00 00 80 11
0020 18 ed d8 e2 c3 55 00 54
0030 58 86 54 dd 29 68 4f 4b
0040 43 9a bc 53 1f a8 4a c8
0050 bd a0 1e b1 53 fe 62 0d
0060 e6 32 e0 1c 06 d2 c4 4a
0070 96 c2 9f 35 12 80
wireshark_Wi-Fi 20VRF60.pcapng
Paquetes: 1415 · Mostrado: 1415 (100.0%)
Perfil: Default
Escribe aquí para buscar
12°C Despejado
ESP
22:41
08-07-2021





11. Compare los tráficos generados (Teoría y wireshark) por los diferentes tipos de escaneos (Full connect, Stealth y XMAS).
    full connect : -sT
    stealth : -sS
    Xmas : -sX

    PREGUNTAR

12. En wireshark filtre los paquetes enviados con su IP de origen e indique el número de paquetes enviados desde su máquina (pregunta k). Haga una captura de pantalla sobre el último paquete capturado por wireshark.

DUDAS

1. ¿Cómo cerrar los puertos/servicios en Windows? (b)
2. ¿Cómo identificar el rango ip de la casa? (“siendo sigiloso”) (f) **LISTO**
3. ¿Qué es y cómo se hace un escaneo full connect? (i) **LISTO**

REFERENCIAS

1. https://nmap.org/book/port-scanning-options.html
2. https://raiolanetworks.es/blog/que-es-una-direccion-ip/
3. https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ipconfig
4. https://www.xatakawindows.com/aplicaciones-windows/estos-pasos-que-tienes-que-dar-para-desactivar-incluso-desinstalar-cortana-windows-10
5. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Open+SSH+6.6.1p1
6. https://www.fermu.com/36-windows/articulos-y-tutoriales/285-seguridad-en-internet-el-comando-netstat-puertos-y-comunicaciones
7. https://httpd.apache.org/security/vulnerabilities_24.html
8.