

UNIVERSIDAD POLITÉCNICA DE JUVENTINO ROSAS

“Comando netstat .”

Docente: Luis Rey Lara González.

Materia: Sistemas telemáticos

Grupo: 5°A

Integrantes:
Lara Valdez Melissa



Índice

➤ Portada	1
➤ Índice	2
➤ Introducción	2
➤ Desarrollo	3
➤ Conclusiones	24
➤ Referencias	24

Introducción

En este documento se explica las herramientas para revisar los puertos activos e inactivos por los cuales se transmite información y los puertos abiertos para las solicitudes. Por ejemplo con la ejecución del comando netstat muestra las conexiones UDP laa cuáles son conexiones que utilizan el Protocolo de Datagramas de Usuario para enviar datos entre las redes de internet, así como las TCP las cuales se refiere a las conexiones que utilizan el Protocolo de Control de Transmisión para enviar datos de los dispositivos a los programas de aplicación, además dicho protocolo divide esos datos en paquetes antes de enviarlos al destino por medio de redes.

Desarrollo

El comando netstat proviene de “network” y “statistics” consiste en un comando que entrega información sobre los puertos y direcciones por los cuales se ejecutan las conexiones TCP y UDP, así como los puertos abiertos para las solicitudes.

Es importante utilizar este comando ya que al tener la ventaja de conocer y comprobar las conexiones entrantes y salientes del ordenador o el servidor establecidas por medio de la IP, indican que puerto se abrió para el intercambio de información y puede existir el problema de que terceros introduzcan un software malicioso en el sistema o bien que un troyano residente en el sistema instale una backdoor para abrir puertos.

Con otras palabras, el comando netstat sirve para encontrar conexiones activas e inactivas con puertos TCP y UDP ,además esto puede ayudar a solucionar problemas relacionados con la red. Cabe mencionar que los servicios del netstat se utilizan por medio de la línea de comandos del sistema. Para ello en la consola de Powershell se ingresan lo siguientes comandos:

- Comando netstat: Muestra todas las conexiones de redes activas.

```
C:\Users\Melissa>netstat
```

Conexiones activas

Proto	Dirección local	Dirección remota	Estado
TCP	192.168.1.78:59191	170-81-162-69:https	ESTABLISHED
TCP	192.168.1.78:59219	ec2-54-147-21-139:https	ESTABLISHED
TCP	192.168.1.78:59220	ec2-54-173-95-250:https	ESTABLISHED
TCP	192.168.1.78:59222	ec2-54-85-252-152:https	ESTABLISHED
TCP	192.168.1.78:59260	ext-189-247-210-19:https	TIME_WAIT
TCP	192.168.1.78:59300	ext-189-247-210-11:https	ESTABLISHED
TCP	192.168.1.78:59310	121:https	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59194	[2603:1030:40c:e::2]:https	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59217	whatsapp-cdn6-shv-02-qro1:https	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59218	rs-in-f188:5228	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59301	g2600-141c-e000-0000-0000-0000-bdf7-d220:https	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59303	g2600-141c-e000-0000-0000-0000-bdf7-d220:https	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59341	del11s05-in-x03:https	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59343	del11s05-in-x03:https	ESTABLISHED

- Comando tasklist | findstr 4508: Muestra la información detallada de la tarea en la salida. Para este caso mostró un archivo que se ubica dentro del directorio de instalación del software Quartus.. El jtag (Joint Test Access Port) es un protocolo de comunicación que va a permitir acceder a los componentes del circuito electrónico para probar, depurar y programar las tarjetas FPGA.

Esto ya que se instala Quartus en el dispositivo de red el cual debe establecer una comunicación con el servidor JTAG para permitir que el servidor JTAG ejecute servicios JTAG.

```
PS C:\Users\Melissa> tasklist | findstr 4508
jtagserver.exe           4508 Services           0      9,852 KB
PS C:\Users\Melissa>
```

- Comando netstat -a: Muestra la tabla de los puertos abiertos, proporcionando información sobre el tipo de protocolo, su IP, la dirección remota y el estado en el que se encuentra dicho puerto.

```
PS C:\Users\Melissa> netstat -a

Conexiones activas

Proto  Dirección local      Dirección remota      Estado
TCP    0.0.0.0:135          DESKTOP-1G4P1UJ:0    LISTENING
TCP    0.0.0.0:445          DESKTOP-1G4P1UJ:0    LISTENING
TCP    0.0.0.0:1309         DESKTOP-1G4P1UJ:0    LISTENING
TCP    0.0.0.0:5040         DESKTOP-1G4P1UJ:0    LISTENING
TCP    0.0.0.0:7070         DESKTOP-1G4P1UJ:0    LISTENING
TCP    0.0.0.0:49664        DESKTOP-1G4P1UJ:0    LISTENING
TCP    0.0.0.0:49665        DESKTOP-1G4P1UJ:0    LISTENING
TCP    0.0.0.0:49666        DESKTOP-1G4P1UJ:0    LISTENING
TCP    0.0.0.0:49667        DESKTOP-1G4P1UJ:0    LISTENING
TCP    0.0.0.0:49668        DESKTOP-1G4P1UJ:0    LISTENING
TCP    0.0.0.0:49669        DESKTOP-1G4P1UJ:0    LISTENING
TCP    169.254.58.254:139   DESKTOP-1G4P1UJ:0    LISTENING
TCP    192.168.1.78:139     DESKTOP-1G4P1UJ:0    LISTENING
TCP    192.168.1.78:59191   170-81-162-69:https  ESTABLISHED
TCP    192.168.1.78:59219   ec2-54-147-21-139:https ESTABLISHED
TCP    192.168.1.78:59220   ec2-54-173-95-250:https ESTABLISHED
TCP    192.168.1.78:59222   ec2-54-85-252-152:https ESTABLISHED
TCP    192.168.1.78:59300   ext-189-247-210-11:https ESTABLISHED
TCP    [::]:135            DESKTOP-1G4P1UJ:0    LISTENING
TCP    [::]:445            DESKTOP-1G4P1UJ:0    LISTENING
TCP    [::]:7070           DESKTOP-1G4P1UJ:0    LISTENING
TCP    [::]:49664          DESKTOP-1G4P1UJ:0    LISTENING
TCP    [::]:49665          DESKTOP-1G4P1UJ:0    LISTENING
TCP    [::]:49666          DESKTOP-1G4P1UJ:0    LISTENING
TCP    [::]:49667          DESKTOP-1G4P1UJ:0    LISTENING
TCP    [::]:49668          DESKTOP-1G4P1UJ:0    LISTENING
TCP    [::]:49669          DESKTOP-1G4P1UJ:0    LISTENING
TCP    [2806:102e:21:f1c6:a056:e944:bce1:393b]:59194 [2603:1030:40c:e::2]:https ESTABLISHED
TCP    [2806:102e:21:f1c6:a056:e944:bce1:393b]:59217 whatsapp-cdn6-shv-02-qro1:https ESTABLISHED
TCP    [2806:102e:21:f1c6:a056:e944:bce1:393b]:59218 rs-in-f188:5228      ESTABLISHED
```

```
TCP [2806:102e:21:f1c6:a056:e944:bce1:393b]:59301 g2600-141c-e000-0000-0000-0000-bdf7-d220:https ESTABLISHED
TCP [2806:102e:21:f1c6:a056:e944:bce1:393b]:59303 g2600-141c-e000-0000-0000-0000-bdf7-d220:https CLOSE_WAIT
TCP [2806:102e:21:f1c6:a056:e944:bce1:393b]:59341 del11s05-in-x03:https ESTABLISHED
TCP [2806:102e:21:f1c6:a056:e944:bce1:393b]:59343 del11s05-in-x03:https TIME_WAIT
TCP [2806:102e:21:f1c6:a056:e944:bce1:393b]:59356 rw-in-f84:https ESTABLISHED
UDP 0.0.0.0:123 *: *
UDP 0.0.0.0:500 *: *
UDP 0.0.0.0:4500 *: *
UDP 0.0.0.0:5050 *: *
UDP 0.0.0.0:5353 *: *
UDP 0.0.0.0:5353 *: *
UDP 0.0.0.0:5353 *: *
UDP 0.0.0.0:5353 *: *
UDP 0.0.0.0:5353 *: *
UDP 0.0.0.0:5355 *: *
UDP 0.0.0.0:49309 0.0.32.14:443
UDP 0.0.0.0:49777 0.0.32.10:443
UDP 0.0.0.0:50001 *: *
UDP 0.0.0.0:55216 0.0.1.103:443
UDP 0.0.0.0:59097 0.0.32.10:443
UDP 0.0.0.0:63194 0.0.32.14:443
UDP 0.0.0.0:64046 *: *
UDP 0.0.0.0:64823 0.0.32.4:443
UDP 0.0.0.0:65206 0.0.32.14:443
UDP 127.0.0.1:1309 127.0.0.1:1309
UDP 127.0.0.1:1900 *: *
UDP 127.0.0.1:52170 127.0.0.1:52170
UDP 127.0.0.1:56165 *: *
UDP 169.254.58.254:137 *: *
UDP 169.254.58.254:138 *: *
UDP 169.254.58.254:1900 *: *
UDP 169.254.58.254:56163 *: *
UDP 192.168.1.78:137 *: *
UDP 192.168.1.78:138 *: *
UDP 192.168.1.78:1900 *: *
```

```
UDP 169.254.58.254:56163 *: *
UDP 192.168.1.78:137 *: *
UDP 192.168.1.78:138 *: *
UDP 192.168.1.78:1900 *: *
UDP 192.168.1.78:56164 *: *
UDP [:]:123 *: *
UDP [:]:500 *: *
UDP [:]:4500 *: *
UDP [:]:5353 *: *
UDP [:]:5353 *: *
UDP [:]:5353 *: *
UDP [:]:5355 *: *
UDP [:]:49309 [2607:f8b0:4012:81d::200e]:443
UDP [:]:49777 [2607:f8b0:4012:81d::200a]:443
UDP [:]:55216 [2a03:2880:f235:1cd:face:b00c:0:167]:443
UDP [:]:59097 [2607:f8b0:4012:81d::200a]:443
UDP [:]:63194 [2607:f8b0:4012:81d::200e]:443
UDP [:]:64046 *: *
UDP [:]:64823 [2607:f8b0:4012:81e::2004]:443
UDP [:]:65206 [2607:f8b0:4012:81d::200e]:443
UDP [:1]:1900 *: *
UDP [:1]:56162 *: *
UDP [fe80::47ff:9c7d:35a2:80fc%9]:1900 *: *
UDP [fe80::47ff:9c7d:35a2:80fc%9]:56160 *: *
UDP [fe80::9657:4b82:2103:41ba%11]:1900 *: *
UDP [fe80::9657:4b82:2103:41ba%11]:56161 *: *
```

- Comando netstat -e: Muestra una tabla de las estadísticas de interfaz de los paquetes recibidos y enviados.

```
PS C:\Users\Melissa> netstat -e
Estadísticas de interfaz
```

	Recibidos	Enviados
Bytes	2510707423	201988717
Paquetes de unidifusión	2217663	715274
Paquetes no de unidifusión	3941	6398
Descartados	0	0
Errores	0	0
Protocolos desconocidos	0	

```
PS C:\Users\Melissa>
```

- Comando netstat -i: Similar al comando netstat -a per este agrega el tiempo del estado en milisegundos.

```
PS C:\Users\Melissa> netstat -i
Conexiones activas
```

Proto	Dirección local	Dirección remota	Estado	Tiempo en estado (ms)
TCP	192.168.1.78:59191	170-81-162-69:https	ESTABLISHED	993361
TCP	192.168.1.78:59219	ec2-54-147-21-139:https	ESTABLISHED	983666
TCP	192.168.1.78:59220	ec2-54-173-95-250:https	ESTABLISHED	983653
TCP	192.168.1.78:59222	ec2-54-85-252-152:https	ESTABLISHED	983647
TCP	192.168.1.78:59360	a23-47-207-160:https	ESTABLISHED	257009
TCP	192.168.1.78:59363	server-3-161-55-49:https	ESTABLISHED	197014
TCP	192.168.1.78:59368	74.119.118.149:https	ESTABLISHED	195948
TCP	192.168.1.78:59370	74.119.118.149:https	ESTABLISHED	195590
TCP	192.168.1.78:59381	207.65.37.179:https	ESTABLISHED	194852
TCP	192.168.1.78:59384	ip-185-184-8-90:https	ESTABLISHED	194676
TCP	192.168.1.78:59404	104.18.29.101:https	ESTABLISHED	186949
TCP	192.168.1.78:59408	74.119.118.149:https	ESTABLISHED	183988
TCP	192.168.1.78:59411	103:https	ESTABLISHED	181585
TCP	192.168.1.78:59412	ext-189-247-203-50:https	ESTABLISHED	181016
TCP	192.168.1.78:59429	server-3-161-13-145:https	ESTABLISHED	168419
TCP	192.168.1.78:59430	server-65-9-121-62:https	ESTABLISHED	167985
TCP	192.168.1.78:59431	server-3-161-53-216:https	ESTABLISHED	167915
TCP	192.168.1.78:59434	143:https	ESTABLISHED	163504
TCP	192.168.1.78:59435	218:https	ESTABLISHED	163113
TCP	192.168.1.78:59437	tzqroa-aa-in-f2:https	ESTABLISHED	161384
TCP	192.168.1.78:59438	104:https	ESTABLISHED	160276

```
PS C:\Users\Melissa>
```

- Comando netstat -n: Visualiza las direcciones IP, las direcciones remotas con los puertos y el estado en el que se encuentran.

PS C:\Users\Melissa> netstat -n

Conexiones activas

Proto	Dirección local	Dirección remota	Estado
TCP	192.168.1.78:59191	69.162.81.170:443	ESTABLISHED
TCP	192.168.1.78:59219	54.147.21.139:443	ESTABLISHED
TCP	192.168.1.78:59220	54.173.95.250:443	ESTABLISHED
TCP	192.168.1.78:59222	54.85.252.152:443	ESTABLISHED
TCP	192.168.1.78:59360	23.47.207.160:443	ESTABLISHED
TCP	192.168.1.78:59363	3.161.55.49:443	ESTABLISHED
TCP	192.168.1.78:59368	74.119.118.149:443	ESTABLISHED
TCP	192.168.1.78:59370	74.119.118.149:443	ESTABLISHED
TCP	192.168.1.78:59381	207.65.37.179:443	ESTABLISHED
TCP	192.168.1.78:59384	185.184.8.90:443	ESTABLISHED
TCP	192.168.1.78:59404	104.18.29.101:443	ESTABLISHED
TCP	192.168.1.78:59408	74.119.118.149:443	ESTABLISHED
TCP	192.168.1.78:59411	34.107.223.103:443	ESTABLISHED
TCP	192.168.1.78:59412	189.247.203.50:443	ESTABLISHED
TCP	192.168.1.78:59429	3.161.13.145:443	ESTABLISHED
TCP	192.168.1.78:59430	65.9.121.62:443	ESTABLISHED
TCP	192.168.1.78:59431	3.161.53.216:443	ESTABLISHED
TCP	192.168.1.78:59434	34.120.107.143:443	ESTABLISHED
TCP	192.168.1.78:59435	34.98.64.218:443	ESTABLISHED
TCP	192.168.1.78:59437	192.178.52.130:443	ESTABLISHED
TCP	192.168.1.78:59438	34.160.138.104:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59194	[2603:1030:40c:e::2]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59217	[2a03:2880:f235:1cd:face:b00c:0:167]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59218	[2607:f8b0:4023:1000:bc]:5228	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59301	[2600:141c:e000:bdfe:d220]:443	CLOSE_WAIT
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59303	[2600:141c:e000:bdfe:d220]:443	CLOSE_WAIT
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59364	[2620:100:a005:d]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59367	[2620:100:a005:d]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59376	[2602:803:c001:200:144]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59383	[2606:4700:10::6816:1fd1]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59405	[2620:100:a005:d]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59406	[2607:f8b0:4012:829::2001]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59413	[2600:141c:e000:bdfe:5139]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59414	[2600:141c:e000:bdfe:51f0]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59416	[2606:4700:10::6816:3556]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59418	[2600:141c:e000:bdfe:51f2]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59423	[2607:f8b0:4012:805::200a]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59424	[2607:f8b0:4012:821::2002]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59425	[2607:f8b0:4001:c00::5e]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59432	[2607:f8b0:4012:80a::2001]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59433	[2607:f8b0:4012:824::2002]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59436	[2607:f8b0:4012:824::2002]:443	ESTABLISHED
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59439	[2607:f8b0:4007:80a::2003]:443	ESTABLISHED

PS C:\Users\Melissa>

- Comando netstat -p protocol: Muestra solo las conexiones para el protocolo especificado (ya sea TCP, UDP, TCPv6 o UDPv6).


```
PS C:\Users\Melissa> netstat -p tcp
```

Conexiones activas

Proto	Dirección local	Dirección remota	Estado
TCP	192.168.1.78:59191	170-81-162-69:https	ESTABLISHED
TCP	192.168.1.78:59219	ec2-54-147-21-139:https	ESTABLISHED
TCP	192.168.1.78:59220	ec2-54-173-95-250:https	ESTABLISHED
TCP	192.168.1.78:59222	ec2-54-85-252-152:https	ESTABLISHED
TCP	192.168.1.78:59411	103:https	ESTABLISHED
TCP	192.168.1.78:59434	143:https	ESTABLISHED
TCP	192.168.1.78:59435	218:https	ESTABLISHED
TCP	192.168.1.78:59438	104:https	ESTABLISHED
TCP	192.168.1.78:59441	ext-189-247-210-19:https	ESTABLISHED

```
PS C:\Users\Melissa>
```

- Comando netstat -q: Muestra las conexiones con el número de puertos que están en escucha, así como los que no se encuentren en ese estado.

PS C:\Users\Melissa> netstat -q

Conexiones activas

Proto	Dirección local	Dirección remota	Estado
TCP	0.0.0.0:135	DESKTOP-1G4P1UJ:0	LISTENING
TCP	0.0.0.0:445	DESKTOP-1G4P1UJ:0	LISTENING
TCP	0.0.0.0:1309	DESKTOP-1G4P1UJ:0	LISTENING
TCP	0.0.0.0:5040	DESKTOP-1G4P1UJ:0	LISTENING
TCP	0.0.0.0:7070	DESKTOP-1G4P1UJ:0	LISTENING
TCP	0.0.0.0:49664	DESKTOP-1G4P1UJ:0	LISTENING
TCP	0.0.0.0:49665	DESKTOP-1G4P1UJ:0	LISTENING
TCP	0.0.0.0:49666	DESKTOP-1G4P1UJ:0	LISTENING
TCP	0.0.0.0:49667	DESKTOP-1G4P1UJ:0	LISTENING
TCP	0.0.0.0:49668	DESKTOP-1G4P1UJ:0	LISTENING
TCP	0.0.0.0:49669	DESKTOP-1G4P1UJ:0	LISTENING
TCP	169.254.58.254:139	DESKTOP-1G4P1UJ:0	LISTENING
TCP	192.168.1.78:139	DESKTOP-1G4P1UJ:0	LISTENING
TCP	192.168.1.78:59191	170-81-162-69:https	ESTABLISHED
TCP	192.168.1.78:59219	ec2-54-147-21-139:https	ESTABLISHED
TCP	192.168.1.78:59220	ec2-54-173-95-250:https	ESTABLISHED
TCP	192.168.1.78:59222	ec2-54-85-252-152:https	ESTABLISHED
TCP	192.168.1.78:59411	103:https	ESTABLISHED
TCP	192.168.1.78:59434	143:https	ESTABLISHED
TCP	192.168.1.78:59435	218:https	ESTABLISHED
TCP	192.168.1.78:59438	104:https	ESTABLISHED
TCP	192.168.1.78:59441	ext-189-247-210-19:https	ESTABLISHED
TCP	0.0.0.0:49863	DESKTOP-1G4P1UJ:0	ENLACE
TCP	0.0.0.0:59191	DESKTOP-1G4P1UJ:0	ENLACE
TCP	0.0.0.0:59219	DESKTOP-1G4P1UJ:0	ENLACE
TCP	0.0.0.0:59220	DESKTOP-1G4P1UJ:0	ENLACE
TCP	0.0.0.0:59222	DESKTOP-1G4P1UJ:0	ENLACE
TCP	0.0.0.0:59411	DESKTOP-1G4P1UJ:0	ENLACE
TCP	0.0.0.0:59434	DESKTOP-1G4P1UJ:0	ENLACE

```
TCP 0.0.0.0:59438 DESKTOP-1G4P1UJ:0 ENLACE
TCP 0.0.0.0:59441 DESKTOP-1G4P1UJ:0 ENLACE
TCP [::]:135 DESKTOP-1G4P1UJ:0 LISTENING
TCP [::]:445 DESKTOP-1G4P1UJ:0 LISTENING
TCP [::]:7070 DESKTOP-1G4P1UJ:0 LISTENING
TCP [::]:49664 DESKTOP-1G4P1UJ:0 LISTENING
TCP [::]:49665 DESKTOP-1G4P1UJ:0 LISTENING
TCP [::]:49666 DESKTOP-1G4P1UJ:0 LISTENING
TCP [::]:49667 DESKTOP-1G4P1UJ:0 LISTENING
TCP [::]:49668 DESKTOP-1G4P1UJ:0 LISTENING
TCP [::]:49669 DESKTOP-1G4P1UJ:0 LISTENING
TCP [2806:102e:21:f1c6:a056:e944:bce1:393b]:59194 [2603:1030:40c:e::2]:https ESTABLISHED
TCP [2806:102e:21:f1c6:a056:e944:bce1:393b]:59217 whatsapp-cdn6-shv-02-qro1:https ESTABLISHED
TCP [2806:102e:21:f1c6:a056:e944:bce1:393b]:59218 rs-in-f188:5228 ESTABLISHED
TCP [2806:102e:21:f1c6:a056:e944:bce1:393b]:59301 g2600-141c-e000-0000-0000-0000-bdf7-d220:https CLOSE_WAIT
TCP [2806:102e:21:f1c6:a056:e944:bce1:393b]:59303 g2600-141c-e000-0000-0000-0000-bdf7-d220:https CLOSE_WAIT
TCP [2806:102e:21:f1c6:a056:e944:bce1:393b]:59376 [2602:803:c001::200:144]:https ESTABLISHED
TCP [::]:59194 DESKTOP-1G4P1UJ:0 ENLACE
TCP [::]:59217 DESKTOP-1G4P1UJ:0 ENLACE
TCP [::]:59218 DESKTOP-1G4P1UJ:0 ENLACE
TCP [::]:59301 DESKTOP-1G4P1UJ:0 ENLACE
TCP [::]:59303 DESKTOP-1G4P1UJ:0 ENLACE
TCP [::]:59376 DESKTOP-1G4P1UJ:0 ENLACE
UDP 0.0.0.0:123 *: *
UDP 0.0.0.0:500 *: *
UDP 0.0.0.0:4500 *: *
UDP 0.0.0.0:5050 *: *
UDP 0.0.0.0:5353 *: *
UDP 0.0.0.0:5353 *: *
UDP 0.0.0.0:5353 *: *
UDP 0.0.0.0:5353 *: *
UDP 0.0.0.0:5353 *: *
UDP 0.0.0.0:5355 *: *
UDP 0.0.0.0:49309 0.0.32.14:443
UDP 0.0.0.0:49777 0.0.32.10:443
```

```

UDP    0.0.0.0:50001      *: *
UDP    0.0.0.0:54455      0.0.32.3:443
UDP    0.0.0.0:57046      *: *
UDP    0.0.0.0:59097      0.0.32.10:443
UDP    0.0.0.0:63194      0.0.32.14:443
UDP    0.0.0.0:63490      0.0.32.10:443
UDP    0.0.0.0:65206      0.0.32.14:443
UDP    127.0.0.1:1309     127.0.0.1:1309
UDP    127.0.0.1:1900     *: *
UDP    127.0.0.1:52170    127.0.0.1:52170
UDP    127.0.0.1:56165    *: *
UDP    169.254.58.254:137 *: *
UDP    169.254.58.254:138 *: *
UDP    169.254.58.254:1900 *: *
UDP    169.254.58.254:56163 *: *
UDP    192.168.1.78:137   *: *
UDP    192.168.1.78:138   *: *
UDP    192.168.1.78:1900   *: *
UDP    192.168.1.78:56164 *: *
UDP    [::]:123           *: *
UDP    [::]:500           *: *
UDP    [::]:4500          *: *
UDP    [::]:5353          *: *
UDP    [::]:5353          *: *
UDP    [::]:5353          *: *
UDP    [::]:5355          *: *
UDP    [::]:49309         [2607:f8b0:4012:81d::200e]:443
UDP    [::]:49777         [2607:f8b0:4012:81d::200a]:443
UDP    [::]:54455         [2607:f8b0:4007:809::2003]:443
UDP    [::]:57046         *: *
UDP    [::]:59097         [2607:f8b0:4012:81d::200a]:443
UDP    [::]:63194         [2607:f8b0:4012:81d::200e]:443
UDP    [::]:63490         [2607:f8b0:4012:813::200a]:443
UDP    [::]:65206         [2607:f8b0:4012:81d::200e]:443
UDP    [::1]:1900         *: *

```

```

UDP    [::1]:56162         *: *
UDP    [fe80::47ff:9c7d:35a2:80fc%9]:546  *: *
UDP    [fe80::47ff:9c7d:35a2:80fc%9]:1900  *: *
UDP    [fe80::47ff:9c7d:35a2:80fc%9]:56160 *: *
UDP    [fe80::9657:4b82:2103:41ba%11]:1900 *: *
UDP    [fe80::9657:4b82:2103:41ba%11]:56161 *: *
C:\Users\Melissa>

```

- Comando netstat -r: Visualiza la tabla de enrutamiento y muestra la lista de las interfaces, tanto IPv4 e IPv6.

PS C:\Users\Melissa> netstat -r

=====

Lista de interfaces

```
14...04 0e 3c 49 ef 27 .....Realtek PCIe GbE Family Controller
9...0a 00 27 00 00 09 .....VirtualBox Host-Only Ethernet Adapter
8...82 91 33 99 5c ab .....Microsoft Wi-Fi Direct Virtual Adapter
4...80 91 33 99 5c ab .....Microsoft Wi-Fi Direct Virtual Adapter #2
11...80 91 33 99 5c ab .....Realtek RTL8723DE 802.11b/g/n PCIe Adapter
1.....Software Loopback Interface 1
```

=====

IPv4 Tabla de enrutamiento

=====

Rutas activas:

Destino de red	Máscara de red	Puerta de enlace	Interfaz	Métrica
0.0.0.0	0.0.0.0	192.168.1.254	192.168.1.78	55
127.0.0.0	255.0.0.0	En vínculo	127.0.0.1	331
127.0.0.1	255.255.255.255	En vínculo	127.0.0.1	331
127.255.255.255	255.255.255.255	En vínculo	127.0.0.1	331
169.254.0.0	255.255.0.0	En vínculo	169.254.58.254	281
169.254.58.254	255.255.255.255	En vínculo	169.254.58.254	281
169.254.255.255	255.255.255.255	En vínculo	169.254.58.254	281
192.168.1.0	255.255.255.0	En vínculo	192.168.1.78	311
192.168.1.78	255.255.255.255	En vínculo	192.168.1.78	311
192.168.1.255	255.255.255.255	En vínculo	192.168.1.78	311
224.0.0.0	240.0.0.0	En vínculo	127.0.0.1	331
224.0.0.0	240.0.0.0	En vínculo	169.254.58.254	281
224.0.0.0	240.0.0.0	En vínculo	192.168.1.78	311
255.255.255.255	255.255.255.255	En vínculo	127.0.0.1	331
255.255.255.255	255.255.255.255	En vínculo	169.254.58.254	281
255.255.255.255	255.255.255.255	En vínculo	192.168.1.78	311

=====

Rutas persistentes:

Ninguno

IPv6 Tabla de enrutamiento

Rutas activas:

	Cuando destino de red métrica	Puerta de enlace
11	71 ::/0	fe80::1
1	331 ::1/128	En vínculo
11	71 2806:102e:21:f1c6::/64	En vínculo
11	311 2806:102e:21:f1c6:a056:e944:bce1:393b/128	En vínculo
11	311 2806:102e:21:f1c6:a46f:195f:c42:eea3/128	En vínculo
11	71 fd00:34fe:df51:e800::/64	En vínculo
11	311 fd00:34fe:df51:e800:8453:aa9a:3ecb:f833/128	En vínculo
11	311 fd00:34fe:df51:e800:a056:e944:bce1:393b/128	En vínculo
9	281 fe80::/64	En vínculo
11	311 fe80::/64	En vínculo
9	281 fe80::47ff:9c7d:35a2:80fc/128	En vínculo
11	311 fe80::9657:4b82:2103:41ba/128	En vínculo
1	331 ff00::/8	En vínculo
9	281 ff00::/8	En vínculo
11	311 ff00::/8	En vínculo

Rutas persistentes:

Ninguno

- Comando netstat -s: Muestra las estadísticas sobre los protocolos importantes.

```
PS C:\Users\Melissa> netstat -s
```

Estadísticas de IPv4

Paquetes recibidos	= 24086
Errores de encabezado recibidos	= 0
Errores de dirección recibidos	= 60
Datagramas reenviados	= 0
Protocolos desconocidos recibidos	= 0
Paquetes recibidos descartados	= 436
Paquetes recibidos procesados	= 26238
Solicitudes de salida	= 25276
Descartes de enrutamiento	= 0
Paquetes de salida descartados	= 5
Paquetes de salida sin ruta	= 7
Reensamblados requeridos	= 0
Reensamblados correctos	= 0
Reensamblados erróneos	= 0
Datagramas correctamente fragmentados	= 0
Datagramas mal fragmentados	= 0
Fragmentos creados	= 0

Estadísticas de IPv6

Paquetes recibidos	= 289689
Errores de encabezado recibidos	= 0
Errores de dirección recibidos	= 277
Datagramas reenviados	= 0
Protocolos desconocidos recibidos	= 0
Paquetes recibidos descartados	= 718
Paquetes recibidos procesados	= 289010
Solicitudes de salida	= 87604
Descartes de enrutamiento	= 0
Paquetes de salida descartados	= 42

```

Paquetes de salida sin ruta      = 19
Reensamblados requeridos       = 0
Reensamblados correctos        = 0
Reensamblados erróneos         = 0
Datagramas correctamente fragmentados = 0
Datagramas mal fragmentados    = 0
Fragmentos creados              = 0

```

Estadísticas ICMPv4

	Recibidos	Enviados	
Mensajes	11	76	
Errores	0	0	
Destino inaccesible	11	76	
Tiempo agotado	0	0	
Problemas de parámetros	0	0	
Paquetes de control de flujo	0	0	
Redirecciones	0	0	
Respuestas de eco	0	0	
Ecos	0	0	
Marcas de tiempo		0	0
Respuestas de marca de tiempo		0	0
Máscaras de direcciones	0	0	
Máscaras de direcciones respondidas	0	0	
Solicitudes de enrutador	0	0	
Anuncios de enrutador	0	0	

Estadísticas de ICMPv6

	Recibidos	Enviados
Mensajes	452	810
Errores	0	0
Destino inaccesible	3	230
Paquete demasiado grande	0	0
Tiempo agotado	0	0

Problemas de parámetros	0	0
Ecos	0	0
Respuestas de eco	0	0
Consultas MLD	0	0
Informes MLD	0	0
Ejecuciones MLD	0	0
Solicitudes de enrutador	0	21
Anuncios de enrutador	12	0
Solicitudes de vecino	390	142
Anuncios de vecino	47	417
Redirecciones	0	0
Renumeraciones de enrutador	0	0

Estadísticas de TCP para IPv4

Activos abiertos	= 1065
Pasivos abiertos	= 0
Intentos de conexión erróneos	= 197
Conexiones restablecidas	= 40
Conexiones actuales	= 3
Segmentos recibidos	= 23122
Segmentos enviados	= 17227
Segmentos retransmitidos	= 3900

Estadísticas de TCP para IPv6

Activos abiertos	= 582
Pasivos abiertos	= 0
Intentos de conexión erróneos	= 31
Conexiones restablecidas	= 88
Conexiones actuales	= 5
Segmentos recibidos	= 37438
Segmentos enviados	= 27832
Segmentos retransmitidos	= 1949

```
Segmentos enviados           = 27832
Segmentos retransmitidos     = 1949

Estadísticas UDP para IPv4

Datagramas recibidos        = 2967
Sin puerto                   = 422
Errores de recepción         = 0
Datagramas enviados         = 3032

Estadísticas UDP para IPv6

Datagramas recibidos        = 251239
Sin puerto                   = 715
Errores de recepción         = 1
Datagramas enviados         = 55792
PS C:\Users\Melissa> |
```

- Comando netstat -p IP: proporciona estadísticas sobre el número de paquetes de entrada y salida, así como errores de entrada y salida que resultan útiles para solucionar problemas de conexiones SLIP (conexiones de línea serie que usan el Protocolo de Internet de Línea Serie (SLIP) para transmitir datagramas IP y se usa para conectar dispositivos a través de puertos serie y módems).

```
PS C:\Users\Melissa> netstat -p ip

Conexiones activas

Proto  Dirección local      Dirección remota      Estado
```

- Comando netstat -s -p icmpv6: Muestra información estadística de IPv6.

```
PS C:\Users\Melissa> netstat -s -p icmpv6
```

Estadísticas de ICMPv6

	Recibidos	Enviados	
Mensajes		483	846
Errores		0	0
Destino inaccesible		3	231
Paquete demasiado grande	0	0	
Tiempo agotado		0	0
Problemas de parámetros		0	0
Ecos		0	0
Respuestas de eco		0	0
Consultas MLD	0	0	
Informes MLD	0	0	
Ejecuciones MLD	0	0	
Solicitudes de enrutador	0	21	
Anuncios de enrutador	13	0	
Solicitudes de vecino	418	148	
Anuncios de vecino	49	446	
Redirecciones		0	0
Renumeraciones de enrutador	0	0	

```
PS C:\Users\Melissa>
```

- Comando netstat -ano: muestran el estado de la red y estadísticas de protocolo.

```
PS C:\Users\Melissa> netstat -ano
```

Conexiones activas

Proto	Dirección local	Dirección remota	Estado	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1100
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1309	0.0.0.0:0	LISTENING	4560
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	4492
TCP	0.0.0.0:7070	0.0.0.0:0	LISTENING	4388
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	976
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	816
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1596
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	1796
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	3700
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	940
TCP	169.254.58.254:139	0.0.0.0:0	LISTENING	4
TCP	192.168.1.78:139	0.0.0.0:0	LISTENING	4
TCP	192.168.1.78:59191	69.162.81.170:443	ESTABLISHED	4388
TCP	192.168.1.78:59220	54.173.95.250:443	ESTABLISHED	1740
TCP	192.168.1.78:59222	54.85.252.152:443	ESTABLISHED	1740
TCP	192.168.1.78:59474	204.79.197.203:443	TIME_WAIT	0
TCP	:::135	:::0	LISTENING	1100
TCP	:::445	:::0	LISTENING	4
TCP	:::7070	:::0	LISTENING	4388
TCP	:::49664	:::0	LISTENING	976
TCP	:::49665	:::0	LISTENING	816
TCP	:::49666	:::0	LISTENING	1596
TCP	:::49667	:::0	LISTENING	1796
TCP	:::49668	:::0	LISTENING	3700
TCP	:::49669	:::0	LISTENING	940
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59194	[2603:1030:40c:e::2]:443	ESTABLISHED	4860
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59217	[2a03:2880:f235:1cd:face:b00c:0:167]:443	ESTABLISHED	1740
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59218	[2607:f8b0:4023:1000::bc]:5228	ESTABLISHED	1740
TCP	[2806:102e:21:f1c6:a056:e944:bce1:393b]:59301	[2600:141c:e000::bdf7:d220]:443	CLOSE_WAIT	6896

```
TCP [2806:102e:21:f1c6:a056:e944:bce1:393b]:59303 [2600:141c:e000::bdf7:d220]:443 CLOSE_WAIT 6896
UDP 0.0.0.0:68 ** 3108
UDP 0.0.0.0:123 ** 10096
UDP 0.0.0.0:500 ** 4504
UDP 0.0.0.0:4500 ** 4504
UDP 0.0.0.0:5050 ** 4492
UDP 0.0.0.0:5353 ** 8936
UDP 0.0.0.0:5353 ** 3036
UDP 0.0.0.0:5353 ** 8936
UDP 0.0.0.0:5353 ** 8936
UDP 0.0.0.0:5353 ** 8936
UDP 0.0.0.0:5355 ** 3036
UDP 0.0.0.0:49463 0.0.32.14:443 1740
UDP 0.0.0.0:50001 ** 4388
UDP 0.0.0.0:50323 0.0.32.10:443 1740
UDP 0.0.0.0:56440 0.0.32.10:443 1740
UDP 0.0.0.0:57221 0.0.32.3:443 1740
UDP 0.0.0.0:58754 0.0.32.14:443 1740
UDP 0.0.0.0:61389 0.0.32.10:443 1740
UDP 127.0.0.1:1309 127.0.0.1:1309 4560
UDP 127.0.0.1:1900 ** 3652
UDP 127.0.0.1:52170 127.0.0.1:52170 4520
UDP 127.0.0.1:56165 ** 3652
UDP 169.254.58.254:137 ** 4
UDP 169.254.58.254:138 ** 4
UDP 169.254.58.254:1900 ** 3652
UDP 169.254.58.254:56163 ** 3652
UDP 192.168.1.78:137 ** 4
UDP 192.168.1.78:138 ** 4
UDP 192.168.1.78:1900 ** 3652
UDP 192.168.1.78:56164 ** 3652
UDP [::]:123 ** 10096
UDP [::]:500 ** 4504
UDP [::]:4500 ** 4504
UDP [::]:5353 ** 8936
```

```
UDP [::]:5353 ** 8936
UDP [::]:5353 ** 3036
UDP [::]:5355 ** 3036
UDP [::]:49463 [2607:f8b0:4012:82a::200e]:443 1740
UDP [::]:50323 [2607:f8b0:4012:81e::200a]:443 1740
UDP [::]:56440 [2607:f8b0:4012:824::200a]:443 1740
UDP [::]:57221 [2607:f8b0:4007:809::2003]:443 1740
UDP [::]:58754 [2607:f8b0:4012:822::200e]:443 1740
UDP [::]:61389 [2607:f8b0:4012:82a::200a]:443 1740
UDP [::1]:1900 ** 3652
UDP [::1]:56162 ** 3652
UDP [fe80::47ff:9c7d:35a2:80fc%9]:1900 ** 3652
UDP [fe80::47ff:9c7d:35a2:80fc%9]:56160 ** 3652
UDP [fe80::9657:4b82:2103:41ba%11]:1900 ** 3652
UDP [fe80::9657:4b82:2103:41ba%11]:56161 ** 3652
```

S C:\Users\Melissa> |

- Comando netstat -u: Muestra menú general de netstat y las opciones que pueden ejecutarse , explicando para qué sirve cada una de ellas.

```
PS C:\Users\Melissa> netstat -u
```

Muestra estadísticas de protocolo y conexiones de red de TCP/IP actuales.

```
NETSTAT [-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]
```

```
-a      Muestra todas las conexiones y los puertos de escucha.
-b      Muestra el ejecutable relacionado con la creación de cada conexión o
        puerto de escucha. En algunos casos bien conocidos, los ejecutables hospedan
        varios componentes independientes y, en estos casos, se muestra la
        secuencia de componentes relacionados con la creación de la conexión
        o el puerto de escucha. En este caso, el nombre del
        ejecutable está entre corchetes, "[ ]", en la parte inferior, encima del componente al que haya llamado,
        y así hasta que se alcance TCP/IP. Ten en cuenta que esta opción
        puede consumir bastante tiempo y dará error si no se dispone de los permisos
        adecuados.
-e      Muestra estadísticas de Ethernet. Esto se puede combinar con la
        opción -s.
-f      Muestra nombres de dominio completos (FQDN) para direcciones
        externas.
-i      Muestra el tiempo gastado por una conexión TCP en su estado actual.
-n      Muestra direcciones y números de puerto en formato numérico.
-o      Muestra el id. del proceso propietario asociado con cada conexión.
-p proto Muestra conexiones para el protocolo especificado por proto; proto
        puede ser cualquiera de los siguientes: TCP, UDP, TCPv6 o UDPv6. Si se usa con la opción -s
        para mostrar estadísticas por protocolo, proto puede ser cualquiera de los siguientes:
        IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-q      Muestra todas las conexiones, puertos de escucha y puertos TCP de enlace
        que no sean de escucha. Los puertos de enlace que no sean de escucha pueden estar o no
        asociados con una conexión activa.
-r      Muestra la tabla de enrutamiento.
-s      Muestra las estadísticas por protocolo. De manera predeterminada, las estadísticas
        se muestran para IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP y UDPv6;
        la opción -p se puede usar para especificar un subconjunto de los valores predeterminados.
-t      Muestra el estado de descarga de la conexión actual.

-x      Muestra conexiones, agentes de escucha y extremos compartidos
        de NetworkDirect.
-y      Muestra la plantilla de conexión TCP para todas las conexiones.
        No se puede combinar con otras opciones.
interval Vuelve a mostrar las estadísticas seleccionadas y realiza pausas en intervalos de varios segundos
        entre cada visualización. Presiona Ctrl+C para que dejen de volver a mostrarse
        las estadísticas. Si se omite, netstat mostrará la
        información de configuración una vez.
```

```
PS C:\Users\Melissa>
```

- Comando netstat -x: muestra simbólicamente el contenido de varias estructuras de datos relacionadas con la red para las conexiones activas.

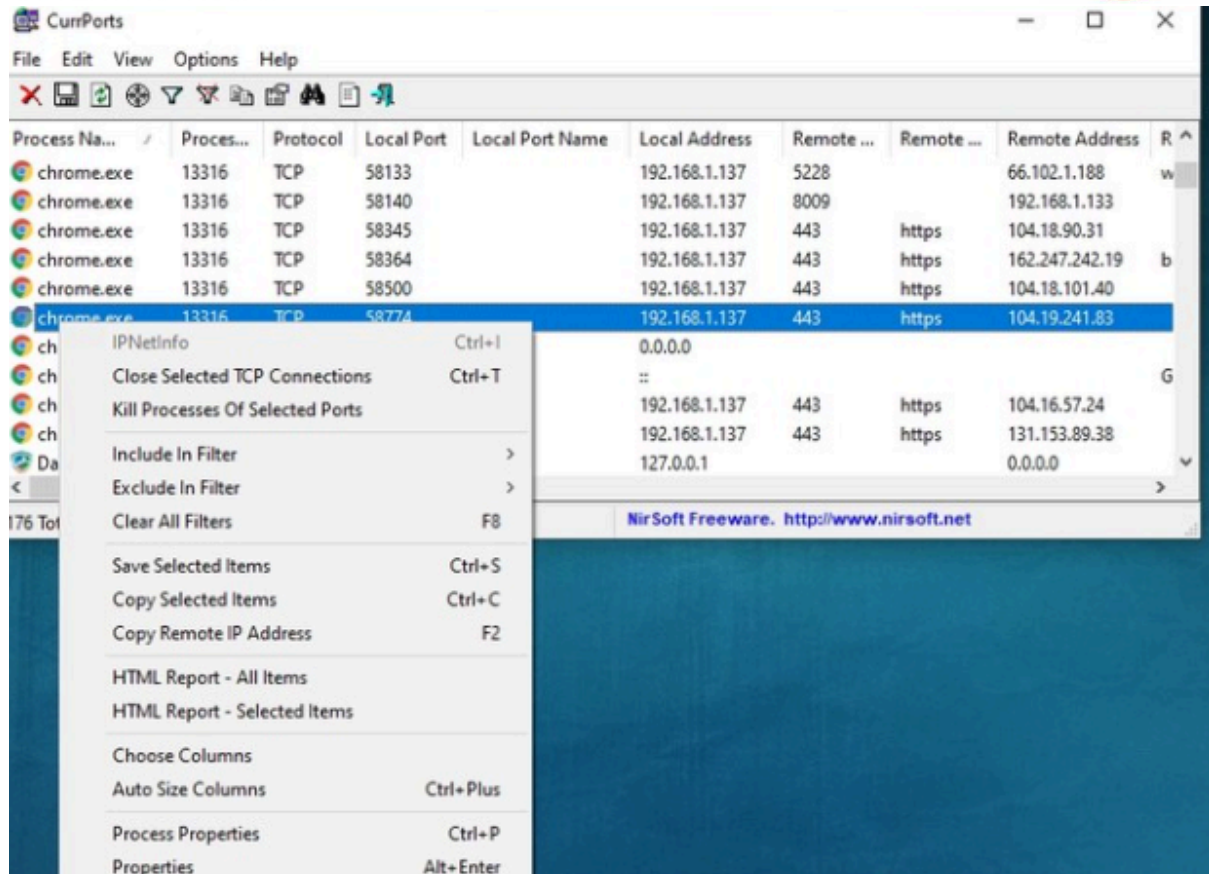
```
PS C:\Users\Melissa> netstat -x
```

Conexiones NetworkDirect activas, escuchas, extremos compartidos

Modo	Tipo	IfIndex	Dirección local	Dirección externa	PID
------	------	---------	-----------------	-------------------	-----

Una segunda opción es utilizar la aplicación **CurrPorts** para visualizar los puertos abiertos, si es un puerto dedicado y su nombre, ya que esta aplicación también te da información avanzada como el número proceso o las direcciones a las que se está conectando cada herramienta.

Además, si se hace click derecho sobre una conexión se mostrará una ventana de opciones donde puedes ver las propiedades del proceso, obtener informes de conexión o cerrar el proceso de los puertos seleccionados.



Estas herramientas de análisis de puertos utilizan tres términos comunes para determinar el estado de los puertos explorados: cerrado, filtrado y abierto.

- Puertos cerrados: Puertos de red que rechazan completamente todos los paquetes dirigidos hacia ellos y no facilitan ningún tráfico entrante o saliente.
- Puertos filtrados: Puertos regulados por agentes de red como los firewalls para control del tráfico de entrada y salida hacia ellos. Cualquier tráfico o paquete no autorizado por el firewall es ignorado o descartado.
- Puertos abiertos: Puerto se considerado abierto cuando hay una aplicación o servicio escuchando en ese puerto y es accesible desde fuera de su red.

Técnicamente, que un puerto esté abierto no es suficiente para que se establezca un canal de comunicación. Para que una entidad externa a su red se comunice con los puertos de red, es necesario que haya una aplicación o servicio escuchando en el puerto. Si no hay ninguno escuchando, entonces todos los paquetes dirigidos a ese puerto se descartan automáticamente.

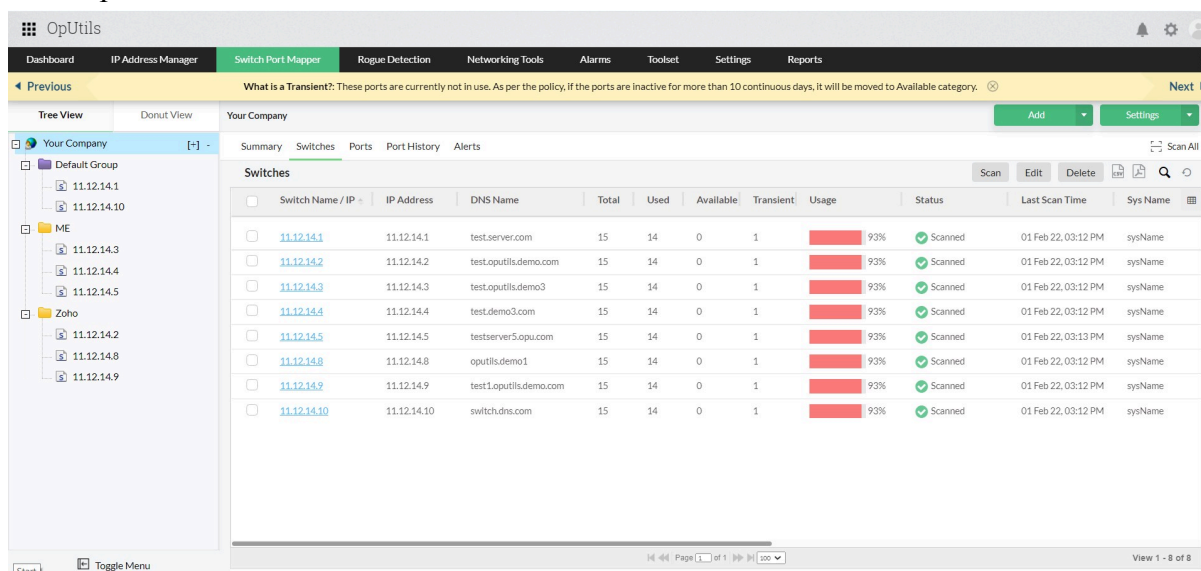
No todos los puertos abiertos con servicios escuchando en ellos exponen su red a vectores de riesgo. De hecho, los dispositivos de red pueden tener algunos puertos como el puerto 21 (FTP), y el puerto 23 (Telnet) abiertos de forma predeterminada.

Un puerto abierto se convierte en el objetivo de los atacantes si existe una vulnerabilidad en la red que les permita ingresar en su sistema y extraer información crítica. Aunque no todos

los servicios que escuchan en un puerto hacen que sea peligroso, cualquier puerto abierto sin supervisión podría estar ejecutando servicios no autorizados, mal configurados o fácilmente explotables por los atacantes. Los atacantes pueden analizar los puertos para identificar fácilmente los puntos vulnerables de la red, lo que puede ayudarles a atacar de forma contundente.

La herramientas que se proponen para cerrar dichos puertos y tener el control y supervisión de ellos son:

- OpUtils que ofrece funciones como la gestión de direcciones IP, que incluye el escaneo de IP avanzado, la detección de dispositivos maliciosos, y más de 30 herramientas de red, incluyendo una herramienta de Wake-on-LAN que ayuda a los administradores de red a escanear y controlar los recursos de la red y solucionar problemas de forma eficiente.



The screenshot shows the OpUtils web interface with the 'Switches' tab selected. It displays a table of network switches with columns for IP Address, DNS Name, Total, Used, Available, Transient, Usage, Status, Last Scan Time, and Sys Name. The table lists 10 switches, all with a status of 'Scanned' and a usage of 93%.

Switch Name / IP	IP Address	DNS Name	Total	Used	Available	Transient	Usage	Status	Last Scan Time	Sys Name
11.12.14.1	11.12.14.1	test.server.com	15	14	0	1	93%	Scanned	01 Feb 22, 03:12 PM	sysName
11.12.14.2	11.12.14.2	test.oputils.demo.com	15	14	0	1	93%	Scanned	01 Feb 22, 03:12 PM	sysName
11.12.14.3	11.12.14.3	test.oputils.demo3	15	14	0	1	93%	Scanned	01 Feb 22, 03:12 PM	sysName
11.12.14.4	11.12.14.4	test.demo3.com	15	14	0	1	93%	Scanned	01 Feb 22, 03:12 PM	sysName
11.12.14.5	11.12.14.5	testserver5.opu.com	15	14	0	1	93%	Scanned	01 Feb 22, 03:13 PM	sysName
11.12.14.8	11.12.14.8	oputils.demo1	15	14	0	1	93%	Scanned	01 Feb 22, 03:12 PM	sysName
11.12.14.9	11.12.14.9	test1.oputils.demo.com	15	14	0	1	93%	Scanned	01 Feb 22, 03:12 PM	sysName
11.12.14.10	11.12.14.10	switchdns.com	15	14	0	1	93%	Scanned	01 Feb 22, 03:12 PM	sysName

- SiteLock: comprueba cada puerto (miles) en el servidor para garantizar que solo los puertos apropiados estén abiertos para el tipo de servidor utilizado (puertos de correo electrónico para los servidores de correo electrónico, los puertos web para servidores web, por ejemplo). Comprueba si se identifica algo inusual, y envía una notificación para corregir el problema pero tiene un costo mensual.



- Windows Powershell, el cortafuegos del servidor host o herramientas como Firewalld e iptables: Para cerrar puertos con Windows Powershell se debe abrir la herramienta de autorización de tareas de Windows Powershell como administrador del sistema y luego escribir el comando **Stop-Process -Id** (Get-NetTCPConnection -LocalPort “puerto”),

después el comando **OwningProcess -Force** y con ello reemplazar el puerto por el número del puerto que se quiera cerrar. Luego se reinicia el ordenador para que los cambios se apliquen.

- Cerrar puertos con el cortafuegos del servidor host: Revisar la lista de puertos abiertos al tráfico del cortafuegos, bloquear los puertos que no sean necesarios.

Conclusiones

Es importante la supervisión de los puertos para evitar robo de información o bien evitar algunas amenazas que pongan en riesgo la seguridad de los dispositivos y la información que se comparte a través de ellos.

Referencias

- Equipo editorial de IONOS. (2023, 1 marzo). Introducción a netstat: ¿qué es netstat y cómo funciona? IONOS Digital Guide.
<https://www.ionos.mx/digitalguide/servidores/herramientas/una-introduccion-a-netstat/>
- Fernández, Y. (2023, 13 diciembre). *Cómo ver los puertos que tienes abiertos en tu ordenador Windows*. Xataka.
<https://www.xataka.com/basics/como-ver-puertos-que-tienes-abiertos-tu-ordenador-windows>
- <https://www.intel.com/content/www/us/en/docs/programmable/683472/21-4/installing-and-configuring-jtagserver.html>
- Jethva, H. (2023, 27 noviembre). *Netstat Command Line Tips and Tricks*. Atlantic.Net.
<https://www.atlantic.net/vps-hosting/netstat-command-line-tips-and-tricks/>
- <https://blogs.manageengine.com/espanol/2021/07/07/descubrimiento-amenazas-puertos-abiertos-htas-analisis-puertos.html>
- <https://soporte.hostgator.mx/hc/es-419/articles/28444244883859-Vulnerabilidades-de-Seguridad-en-la-Red#:~:text=%C2%BFQue%20puedo%20hacer%20al%20respecto,c%20omo%20SiteLock%20Premium%2C%20por%20ejemplo.>
- https://www.sailpoint.com/es/products/identity-security-cloud/atlas/add-ons/data-access-security?igaag=152595782061&igaat=&igacm=20779288968&igacr=725627249178&igakw=seguridad%20de%20acceso%20a%20datos&igamt=p&igant=g&campaignid=20779288968&utm_source=google&utm_network=g&utm_medium=cpc&utm_content=ams-es-das&utm_term=seguridad%20de%20acceso%20a%20datos&utm_id=7012J000001Fba9&gad_source=1&gclid=CjwKCAiAneK8BhAVEiwAoy2HYQ_X2Loo6Qw6_L7NTkYjgfnJt9Bf7Ex8H8D5kWcuJC5n2-3Lspi30xoCAeoQAvD_BwE
- <https://www.hostinger.mx/tutoriales/protocolo-tcp>
- <https://www.adslzone.net/esenciales/windows-10/abrir-puertos-firewall/#543580-en-windows-10>