Laboratorio No. 3 - Escaneo de Puertos

ALEXANDER VILLATORO 1182118

Objetivo

a) Reconocer los dispositivos que se encuentran en una Red.
b) Identificar que puertos y servicios están disponibles

1. Identifique sus datos de red
   a. Dirección IP

```
   IPv4 Address. . . . . . . . . . . : 192.168.1.7
```

   b. DNS

```
Connection-specific DNS Suffix  . :
```

   c. Gateway.

```
Default Gateway . . . . . . . . . : fe80::763a:efff:feb5:7970%9
                                    192.168.1.1
```

2. Ejecute el comando Netststat : netstat -na
   a. Identifique que puertos están:
      i. escuchando por conexiones.

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2382	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6646	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING
TCP	0.0.0.0:8391	0.0.0.0:0	LISTENING
TCP	0.0.0.0:8733	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49675	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49676	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3213	0.0.0.0:0	LISTENING
TCP	127.0.0.1:5354	0.0.0.0:0	LISTENING
TCP	127.0.0.1:6463	0.0.0.0:0	LISTENING
TCP	127.0.0.1:49670	0.0.0.0:0	LISTENING

      ii. Conexiones activas y cerradas

```
TCP    127.0.0.1:53198        127.0.0.1:56276        TIME_WAIT
TCP    127.0.0.1:53204        127.0.0.1:56276        CLOSE_WAIT
TCP    127.0.0.1:53205        127.0.0.1:56276        ESTABLISHED
TCP    127.0.0.1:56087        127.0.0.1:65001        ESTABLISHED
TCP    127.0.0.1:56276        0.0.0.0:0              LISTENING
TCP    127.0.0.1:56276        127.0.0.1:53197        TIME_WAIT
TCP    127.0.0.1:56276        127.0.0.1:53204        FIN_WAIT_2
TCP    127.0.0.1:56276        127.0.0.1:53205        ESTABLISHED
TCP    127.0.0.1:56276        127.0.0.1:56290        ESTABLISHED
TCP    127.0.0.1:56276        127.0.0.1:62131        TIME_WAIT
TCP    127.0.0.1:56290        127.0.0.1:56276        ESTABLISHED
TCP    127.0.0.1:62132        127.0.0.1:56276        TIME_WAIT
TCP    127.0.0.1:65001        0.0.0.0:0              LISTENING
TCP    127.0.0.1:65001        127.0.0.1:56087        ESTABLISHED
TCP    192.168.1.7:139        0.0.0.0:0              LISTENING
TCP    192.168.1.7:49257      52.109.16.5:443        TIME_WAIT
TCP    192.168.1.7:49398      8.28.7.81:443          ESTABLISHED
TCP    192.168.1.7:49747      52.114.133.198:443     ESTABLISHED
TCP    192.168.1.7:50124      184.84.152.252:443     ESTABLISHED
TCP    192.168.1.7:50251      162.159.129.233:443    ESTABLISHED
TCP    192.168.1.7:50982      162.159.129.233:443    TIME_WAIT
TCP    192.168.1.7:51112      13.107.6.254:443       ESTABLISHED
TCP    192.168.1.7:51114      131.253.33.254:443     ESTABLISHED
TCP    192.168.1.7:51115      162.159.135.232:443    ESTABLISHED
TCP    192.168.1.7:51117      162.159.135.234:443    ESTABLISHED
TCP    192.168.1.7:51129      162.159.129.235:443    ESTABLISHED
TCP    192.168.1.7:51174      192.65.229.43:443      ESTABLISHED
TCP    192.168.1.7:51177      104.36.113.17:443      ESTABLISHED
TCP    192.168.1.7:51182      107.178.244.119:443    ESTABLISHED
TCP    192.168.1.7:51460      104.36.113.17:443      ESTABLISHED
TCP    192.168.1.7:52712      52.226.139.180:443     ESTABLISHED
TCP    192.168.1.7:52721      54.85.80.8:443         ESTABLISHED
TCP    192.168.1.7:53192      35.186.220.184:443     ESTABLISHED
TCP    192.168.1.7:53206      52.109.12.118:443      ESTABLISHED
TCP    192.168.1.7:53258      172.217.3.130:443      TIME_WAIT
TCP    192.168.1.7:53464      52.10.200.18:8883      ESTABLISHED
TCP    192.168.1.7:53572      52.109.16.5:443        TIME_WAIT
TCP    192.168.1.7:53582      104.94.108.49:443      ESTABLISHED
TCP    192.168.1.7:54199      185.184.8.65:443       ESTABLISHED
TCP    192.168.1.7:54254      23.210.142.147:443     ESTABLISHED
TCP    192.168.1.7:55160      35.186.253.211:443     ESTABLISHED
TCP    192.168.1.7:56398      184.84.152.252:443     ESTABLISHED
TCP    192.168.1.7:56614      107.178.244.119:443    TIME_WAIT
TCP    192.168.1.7:57195      151.101.205.44:443     ESTABLISHED
TCP    192.168.1.7:57299      35.211.233.246:443     ESTABLISHED
TCP    192.168.1.7:57447      184.25.52.223:443      ESTABLISHED
TCP    192.168.1.7:57613      185.199.109.153:443    ESTABLISHED
```

iii. Conexciones cerradas.

b. Puede identificar que aplicación esta asociada a cada puerto?

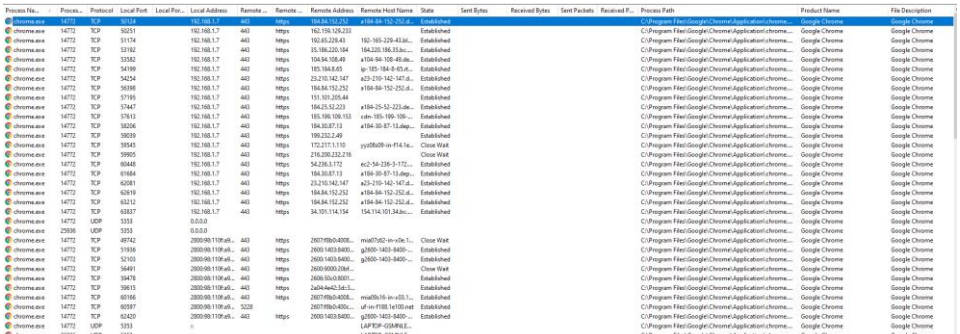
Se puede utilizar el netstat -ab para poder obtener información de que app se está utilizando y en que puerto.

```
C:\WINDOWS\system32>netstat -ab

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            LAPTOP-GSMNLECH:0      LISTENING
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            LAPTOP-GSMNLECH:0      LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:2382           LAPTOP-GSMNLECH:0      LISTENING
 [sqlbrowser.exe]
  TCP    0.0.0.0:5040           LAPTOP-GSMNLECH:0      LISTENING
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:6646           LAPTOP-GSMNLECH:0      LISTENING
 [MMSSHOST.EXE]
  TCP    0.0.0.0:7680           LAPTOP-GSMNLECH:0      LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:8391           LAPTOP-GSMNLECH:0      LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:8733           LAPTOP-GSMNLECH:0      LISTENING
 [HPJumpStartBridge.exe]
  TCP    0.0.0.0:49664          LAPTOP-GSMNLECH:0      LISTENING
 [lsass.exe]
  TCP    0.0.0.0:49665          LAPTOP-GSMNLECH:0      LISTENING
  TCP    127.0.0.1:49670        LAPTOP-GSMNLECH:0      LISTENING
 [CueLLAccessService.exe]
  TCP    127.0.0.1:56087        LAPTOP-GSMNLECH:65001  ESTABLISHED
 [nvcontainer.exe]
  TCP    127.0.0.1:56276        LAPTOP-GSMNLECH:0      LISTENING
 [NVIDIA Web Helper.exe]
  TCP    127.0.0.1:56276        LAPTOP-GSMNLECH:56290  ESTABLISHED
 [NVIDIA Web Helper.exe]
  TCP    127.0.0.1:56290        LAPTOP-GSMNLECH:56276  ESTABLISHED
 [NVIDIA Share.exe]
  TCP    127.0.0.1:65001        LAPTOP-GSMNLECH:0      LISTENING
 [nvcontainer.exe]
  TCP    127.0.0.1:65001        LAPTOP-GSMNLECH:56087  ESTABLISHED
 [nvcontainer.exe]
  TCP    192.168.1.7:139        LAPTOP-GSMNLECH:0      LISTENING
 Can not obtain ownership information
  TCP    192.168.1.7:49222      126:https              ESTABLISHED
 [chrome.exe]
  TCP    192.168.1.7:49677      8.28.7.81:https        ESTABLISHED
 [chrome.exe]
  TCP    192.168.1.7:50092      104.18.100.194:https   ESTABLISHED
 [chrome.exe]
  TCP    192.168.1.7:50953      static:https           ESTABLISHED
 [chrome.exe]
```

3. Ejecute el programa CurrPorts: https://www.nirsoft.net/utils/cports.html
   a. Identifique que servicios están ejecutando en su computador personal.



b. Identifique los puertos y las aplicaciones asociadas.

Process Na...	Proces...	Protocol	Local Port
chrome.exe	14772	TCP	51174
chrome.exe	14772	TCP	54199
chrome.exe	14772	TCP	57195
chrome.exe	14772	TCP	57613
chrome.exe	14772	TCP	59039
chrome.exe	14772	TCP	59545
chrome.exe	14772	TCP	60448
chrome.exe	14772	UDP	5353
chrome.exe	25936	UDP	5353
chrome.exe	14772	TCP	49742
chrome.exe	14772	TCP	59478
chrome.exe	14772	TCP	59615
chrome.exe	14772	TCP	60597
chrome.exe	14772	UDP	5353
chrome.exe	25936	UDP	5353
chrome.exe	14772	UDP	62725
chrome.exe	14772	UDP	62725

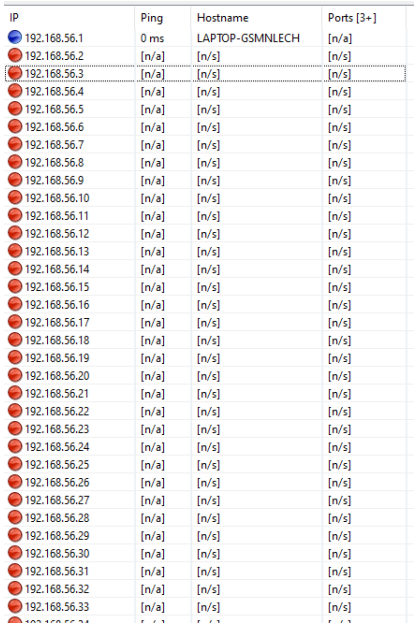
Discord.exe	21760	TCP	6463
Discord.exe	24236	TCP	51115
Discord.exe	24236	TCP	51117
Discord.exe	24236	TCP	51129
Discord.exe	24236	TCP	63037
Discord.exe	24236	TCP	51120
Discord.exe	24236	TCP	51121
Discord.exe	21760	UDP	52528
Discord.exe	24236	TCP	60218
Discord.exe	21760	UDP	60435
Discord.exe	21760	UDP	57273

nvcontainer.exe	5284	UDP	10031
nvcontainer.exe	28424	UDP	51549
nvcontainer.exe	5012	UDP	55085
nvcontainer.exe	5012	UDP	5353
nvcontainer.exe	5012	UDP	55086
NVIDIA Share....	15104	TCP	56290
NVIDIA Share....	15104	TCP	49969
NVIDIA Share....	15104	TCP	49982
NVIDIA Share....	15104	TCP	49983
NVIDIA Web H...	23604	TCP	56276
NVIDIA Web H...	23604	TCP	56276
NVIDIA Web H...	23604	UDP	10030
NVIDIA Web H...	23604	TCP	56276
NVIDIA Web H...	23604	TCP	56276

c. Cuál es la principal diferencia entre netstat y curports?

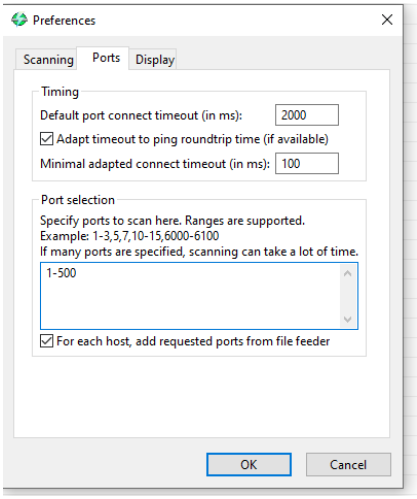
**Netstat es un modo estándar que informa sobre todas las conexiones de red activas, y curports es un software de monitoreo de red que muestra la lista de todos los puertos TCP/IP y UDP abiertos actualmente en su computadora local. **

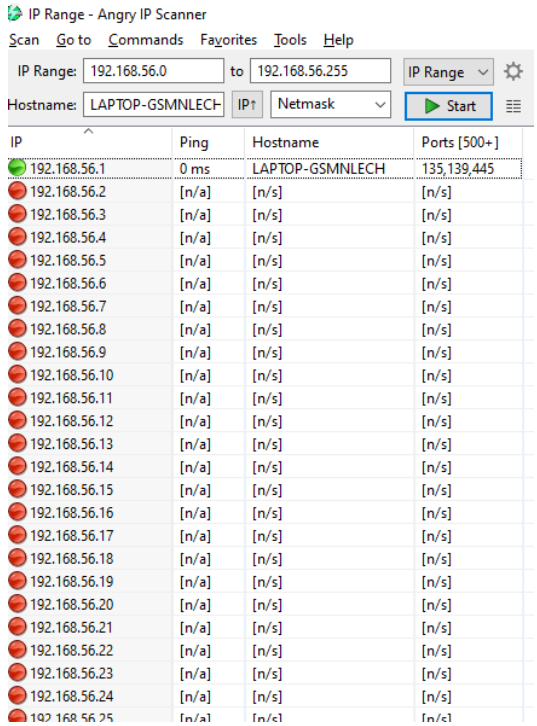
4. Ejecute el programa Angry IP Scanner
    a. Haga un barrido de la red en la que se encuentra.

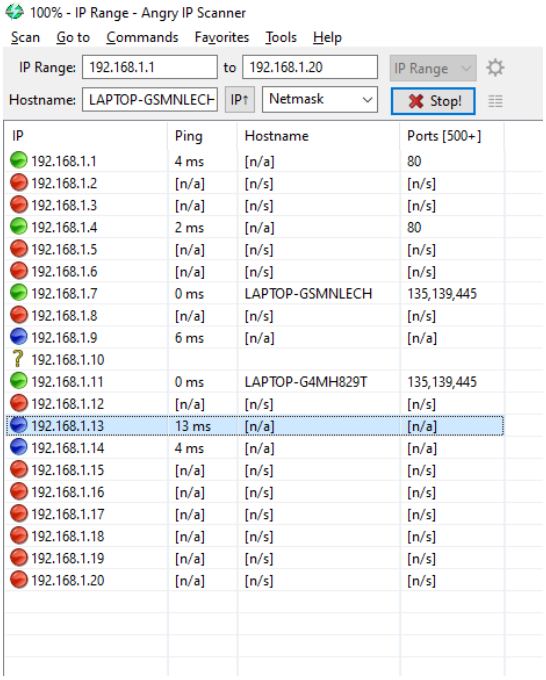


IP	Ping	Hostname	Ports [3+]
192.168.56.1	0 ms	LAPTOP-GSMNLECH	[n/a]
192.168.56.2	[n/a]	[n/s]	[n/s]
192.168.56.3	[n/a]	[n/s]	[n/s]
192.168.56.4	[n/a]	[n/s]	[n/s]
192.168.56.5	[n/a]	[n/s]	[n/s]
192.168.56.6	[n/a]	[n/s]	[n/s]
192.168.56.7	[n/a]	[n/s]	[n/s]
192.168.56.8	[n/a]	[n/s]	[n/s]
192.168.56.9	[n/a]	[n/s]	[n/s]
192.168.56.10	[n/a]	[n/s]	[n/s]
192.168.56.11	[n/a]	[n/s]	[n/s]
192.168.56.12	[n/a]	[n/s]	[n/s]
192.168.56.13	[n/a]	[n/s]	[n/s]
192.168.56.14	[n/a]	[n/s]	[n/s]
192.168.56.15	[n/a]	[n/s]	[n/s]
192.168.56.16	[n/a]	[n/s]	[n/s]
192.168.56.17	[n/a]	[n/s]	[n/s]
192.168.56.18	[n/a]	[n/s]	[n/s]
192.168.56.19	[n/a]	[n/s]	[n/s]
192.168.56.20	[n/a]	[n/s]	[n/s]
192.168.56.21	[n/a]	[n/s]	[n/s]
192.168.56.22	[n/a]	[n/s]	[n/s]
192.168.56.23	[n/a]	[n/s]	[n/s]
192.168.56.24	[n/a]	[n/s]	[n/s]
192.168.56.25	[n/a]	[n/s]	[n/s]
192.168.56.26	[n/a]	[n/s]	[n/s]
192.168.56.27	[n/a]	[n/s]	[n/s]
192.168.56.28	[n/a]	[n/s]	[n/s]
192.168.56.29	[n/a]	[n/s]	[n/s]
192.168.56.30	[n/a]	[n/s]	[n/s]
192.168.56.31	[n/a]	[n/s]	[n/s]
192.168.56.32	[n/a]	[n/s]	[n/s]
192.168.56.33	[n/a]	[n/s]	[n/s]

    b. Modifique el parámetro de puertos, coloque rango desde 1 hasta 500




IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 192.168.56.0 to 192.168.56.255 IP Range
Hostname: LAPTOP-GSMNLECH IP↑ Netmask Start
IP Ping Hostname Ports [500+]
192.168.56.1 0 ms LAPTOP-GSMNLECH 135,139,445
192.168.56.2 [n/a] [n/s] [n/s]
192.168.56.3 [n/a] [n/s] [n/s]
192.168.56.4 [n/a] [n/s] [n/s]
192.168.56.5 [n/a] [n/s] [n/s]
192.168.56.6 [n/a] [n/s] [n/s]
192.168.56.7 [n/a] [n/s] [n/s]
192.168.56.8 [n/a] [n/s] [n/s]
192.168.56.9 [n/a] [n/s] [n/s]
192.168.56.10 [n/a] [n/s] [n/s]
192.168.56.11 [n/a] [n/s] [n/s]
192.168.56.12 [n/a] [n/s] [n/s]
192.168.56.13 [n/a] [n/s] [n/s]
192.168.56.14 [n/a] [n/s] [n/s]
192.168.56.15 [n/a] [n/s] [n/s]
192.168.56.16 [n/a] [n/s] [n/s]
192.168.56.17 [n/a] [n/s] [n/s]
192.168.56.18 [n/a] [n/s] [n/s]
192.168.56.19 [n/a] [n/s] [n/s]
192.168.56.20 [n/a] [n/s] [n/s]
192.168.56.21 [n/a] [n/s] [n/s]
192.168.56.22 [n/a] [n/s] [n/s]
192.168.56.23 [n/a] [n/s] [n/s]
192.168.56.24 [n/a] [n/s] [n/s]


100% - IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 192.168.1.1 to 192.168.1.20 IP Range
Hostname: LAPTOP-GSMNLECH IP↑ Netmask Stop!
IP Ping Hostname Ports [500+]
192.168.1.1 4 ms [n/a] 80
192.168.1.2 [n/a] [n/s] [n/s]
192.168.1.3 [n/a] [n/s] [n/s]
192.168.1.4 2 ms [n/a] 80
192.168.1.5 [n/a] [n/s] [n/s]
192.168.1.6 [n/a] [n/s] [n/s]
192.168.1.7 0 ms LAPTOP-GSMNLECH 135,139,445
192.168.1.8 [n/a] [n/s] [n/s]
192.168.1.9 6 ms [n/a] [n/a]
192.168.1.10
192.168.1.11 0 ms LAPTOP-G4MH829T 135,139,445
192.168.1.12 [n/a] [n/s] [n/s]
192.168.1.13 13 ms [n/a] [n/a]
192.168.1.14 4 ms [n/a] [n/a]
192.168.1.15 [n/a] [n/s] [n/s]
192.168.1.16 [n/a] [n/s] [n/s]
192.168.1.17 [n/a] [n/s] [n/s]
192.168.1.18 [n/a] [n/s] [n/s]
192.168.1.19 [n/a] [n/s] [n/s]
192.168.1.20 [n/a] [n/s] [n/s]

c. Seleccione 1 dirección IP de las que encontró, y haga el barrido nuevamente.
   a. Que puede determinar con la aplicación.

IP	Ping	Hostname	Ports [500+]
192.168.56.1	0 ms	LAPTOP-GSMNLECH	135,139,445

   b. Logro realizar el escaneo.
      Si
   c. Realice el escaneo en una red fuera de la universidad y analice los resultados.

5. Ejecute NMAP
   a. Haga un escaneo de puertos a una IP que está en la red

```
alexander@avR:~/Desktop$ nmap 192.168.1.13
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-28 11:49 CST
Nmap scan report for 192.168.1.13
Host is up (0.0076s latency).
All 1000 scanned ports on 192.168.1.13 are closed

Nmap done: 1 IP address (1 host up) scanned in 21.18 seconds
alexander@avR:~/Desktop$
```

   b. Cuál es la principal diferencia entre nmap y Angry.

      Angry es un programa en el cual se puede hacer un escaneo de puertos, en el caso de nmap se puede hacer de la misma forma ya que tiene un programa en el cual se puede escanear los puertos, la diferencia es que nmap también se puede escanear con comandos desde la terminal.

   c. Logro realizar el escaneo.
      Si, sin ningún problema
   d. Realice el escaneo en una red fuera de la universidad y analice los resultados.