

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
1	TCP	0.0.0.0:2382	0.0.0.0:0	LISTENING
ı	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
1	TCP	0.0.0.0:8391	0.0.0.0:0	LISTENING
į	TCP	0.0.0.0:8733	0.0.0.0:0	LISTENING
	TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
ı	TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
١	TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING
ı	TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING
1	TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING
1	TCP	0.0.0.0:49675	0.0.0.0:0	LISTENING
ı	TCP	0.0.0.0:49676	0.0.0.0:0	LISTENING
	TCP	127.0.0.1:3213	0.0.0.0:0	LISTENING
1	TCP	127.0.0.1:5354	0.0.0.0:0	LISTENING
Į	TCP	127.0.0.1:6463	0.0.0.0:0	LISTENING
1	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 192.168.1.7:53582	52.109.16.5:443	TIME_WAIT
TCP	192.168.1.7:54199	104.94.108.49:443 185.184.8.65:443	ESTABLISHED
TCP TCP	192.168.1.7:54254	23.210.142.147:443	ESTABLISHED 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
ICF	132:100:1:7:37013	109.199.109.199.443	LOTABLIBITED

- 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:\WINDO	WS\system32>netsta	t -ab	
Active C	onnections		
	Local Address	Foreign Address	
	0.0.0.0:135	LAPTOP-GSMNLECH:	0 LISTENING
RpcSs			
[svchos	t.exe] 0.0.0.0:445	LARTOR COMMISCIL	O LICTENING
			0 LISTENING
	obtain ownership : 0.0.0.0:2382	LAPTOP-GSMNLECH:	A LICTUALING
	wser.exe]	LAPTOP-GSMINLECH:	6 LISTENING
		LAPTOP-GSMNLECH:	A LISTENING
CDPSvc		LAPTOP-GSPINLECH.	6 LISTENING
[svchos			
	0.0.0.0:6646	LAPTOP-GSMNLECH:	0 LISTENING
[MMSSHO		EALTOI GSTINEECIT.	LISTENING
	0.0.0.0:7680	LAPTOP-GSMNLECH:	0 LISTENING
	obtain ownership :		E E E E E E E E E E E E E E E E E E E
	0.0.0.0:8391		0 LISTENING
Can not	obtain ownership :	information	
	0.0.0.0:8733	LAPTOP-GSMNLECH:	0 LISTENING
[HPJump	StartBridge.exe]		
TCP	0.0.0.0:49664	LAPTOP-GSMNLECH:	0 LISTENING
[lsass.	exe]		
TCP	0.0.0.0:49665	LAPTOP-GSMNLECH:	0 LISTENING
TCP 1	27.0.0.1:49670	LAPTOP-GSMNLECH:0	LISTENING
	essService.exe]		
TCP 1	27.0.0.1:56087	LAPTOP-GSMNLECH:65001	ESTABLISHED
[nvcontai			
		LAPTOP-GSMNLECH:0	LISTENING
	leb Helper.exe] .27.0.0.1:56276	LAPTOP-GSMNLECH: 56290	ESTABLITSHED
	Meb Helper.exel	EAF TOF -GSHINEECHT. 30290	ESTABLISHED
		LAPTOP-GSMNLECH: 56276	ESTABLISHED
[NVIDIA S	hare.exe]		
		LAPTOP-GSMNLECH:0	LISTENING
[nvcontai		LARTOR COMMUNICAL ECONT	COTABL TOUCH
TCP 1		LAPTOP-GSMNLECH: 56087	ESTABLISHED
	.92.168.1.7:139	LAPTOP-GSMNLECH:0	LISTENING
	btain ownership info		
	92.168.1.7:49222		ESTABLISHED
[chrome.e			
		8.28.7.81:https	ESTABLISHED
[chrome.e		104 10 100 104	ECTADI TOUED
[chrome.e		104.18.100.194:https	ESTABLISHED
	.92.168.1.7:50953	static:https	ESTABLISHED
[chrome.e			

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

rocess Ne.	Proces.	Protocol	Local Port Local P	ov Local Address	Remote	Semote_	Remote Address	Remote Host Name	State	Sent Bytes	Received Bytes	Sent Packets Re	ceived P	Process Path	Product Name	File Description
chrome.exe	14072	TCP	50124	192,168.1,7	40	hetps	184.84.152.252	#184-84-152-252.d.	Established					C/\Program Filed/Google\Chrome\Application\chrome	Google Chrome	Google Chram
chrome.ese	14772	TCP	50251	192.168.1.7	46	https	162.159.129.233		Established					C:\Program Files\Google\Chrome\Application\chrome	Google Chrome	Google Chrom
chroms.ese	14772	TCP	51174	192.168.1.7	443	https	192.65.229.43	192-165-229-43.34	Established					C/Program Files/Google/Chrome/Application/chrome	Google Chrome	Google Chrom
chrome.ese	14772	TCP	53102	192.168.1.7	443	https	35,186,220,184	184.220.186.35.bc	Established					C/Program Files/Google) Chrome/Application/chrome	Google Chrome	Google Chrom
chrome.exe	14772	RCP	53582	192,168,1,7	443	https	104.94.108.49	a104-54-108-49.de.	Established					C/Program Files/Google/Chrome/Application/chrome	Google Chrome	Google Chrom
dirame.ere	14772	TCP	54199	192.168.1.7	443	https	185.184.5.65	ip-185-184-8-65.rt	Established					C/\Program Files\Google\Chrome\Application\chrome	Google Chrome	Google Chrom
chrome.ere	14772	TCP	54254	192.168.1.7	443	https	23,210,142,147	a23-210-142-147.d.,	Established					C/Program Files/Google/Chrome/Application/chrome	Google Chrome	Google Chrom
chrome.ere	14772	TCP	56396	192,168,1.7	443	https	184.84.152.252	#184-84-152-252.d	Established					C/\Program Files\Google\Chrome\Application\chrome	Google Chrome	Google Chrom
chrome.exe	14772	TCP	57195	192.168.1.7	443	https	151,101,205,44		Established					C/Program Files/Google/Chrome/Application/chrome	Google Chrome	Google Chrom
chrame.eue	14772	TCP	57447	192.168.1.7	443	https	184.25.52.223	a184-25-52-223.de	Established					C/Program Filed/Google/Chrome/Application/chrome	Google Chrome	Google Chrom
chrome.ese	14772	TCP	57613	192.168.1.7	46	https	185.199.109.153	cdn-185-199-109	Established					C//Program Files/Google)/Chrome/Application/chrome	Google Chrome	Google Chrom
chrome.ese	14772	TCP	58206	192,168.1.7	46	https	184.30.87.13	a184-30-87-13.dep	Established					C:\Program Files\Google\Chrome\Application\chrome	Google Chrome	Google Chrom
chrome.exe	14772	TCP.	59039	192,168.1.7	443	Pettps	199,232,2,49		Established					C/\Program Files\Google\Chrome\Application\chrome	Google Chrome	Google Chrom
chrome.exe	14772	TCP	29545	192,163.1.7	443	https	172,217,1,110	yyz08x09-in-f14.1e	Close Wait					C/Program Files/Google/Chrome/Application/chrome	Google Chrome	Google Chron
chrome.ere	14772	TCP	59905	192,168,1.7	443	https	216.200.232.216		Close Walt					C/\Program Files\Google\Chrome\Application\chrome	Google Chrome	Google Chron
chrome.eie	14772	TOP	60446	192,168,1.7	443	https	54.236.3.172	ec2-54-236-3-172	Established					C/\Program Files\iGoogle\Chrome\Application\chrome	Google Chrome	Google Chron
chrome.exe	14772	TCP	61684	192.168.1.7	443	https	164.30.87.13	a184-30-87-13.dep	Established					C/Program Files!/Google)/Chromel/Application!.chrome	Google Chrome	Google Chron
chrome-exe	14772	TCP	62081	192.168.1.7	443	https	23.210.142.147	#23-210-142-147.d.	Established					C1Program Filesi Googlei Chromei Application I chrome	Google Chrome	Google Chron
chrome.eve	14772	TCP	62619	192.163.1.7	443	https	184.84.152.252	#184-84-152-252.d.	Established					C:\Program Files Google\Chrome\Application chrome	Google Chrome	Google Chron
chrome.ese	14772	TCP	63212	192.168.1.7	443	https	184.84.152,252	#184-84-152-252.d.	Established					C:\Program Files\Google\Chrome\Application\chrome	Google Chrome	Google Chron
chrome.ese	14772	TCP	63837	192.168.1.7	443	https	34.101.114.154	154.114.101.34.bc	Established					C:\Program Files\Google\Chrome\Application\chrome	Google Chrome	Google Chron
chrome.exe	14772	UDP	2323	0.0.0.0										C/Program Files/Google/Chrome/Application/chrome	Google Chrome	Google Chron
chrome.exe	25936	UDP	5353	0.0.0.0										C//Program Files/IGoogle//Chrome/Application/chrome	Google Chrome	Google Chrom
chromeeie	14772	TCP	49742	2800.98.110ha9.	443	https	2607/950-4006	mia07st2-in-x0e.1	Close Wait					C/Program Files/Google/Chrome/Application/chrome	Google Chrome	Google Chron
chrome.exe	14772	TCP	51916	2000:98:110ha/k.	443	https	2600.1403.8400	g2600-1403-8400	Established					C/\Program Files\Google\Chrome\Application\chrome	Google Chrome	Google Chron
chrome.eue	14772	TCP	52103	2000:90:110Ea9	443	https	2600:1403:8400	g2600-1403-8400	Established					C/Program Files/Google/Chrome/Application/chrome	Google Chrome	Google Chron
chrome.eue	14772	TCP	56491	2800-98-110Ea/L	463	https	2600:9000:20bf		Clone Wait					C:\Program Files Google Chrome\Application chrome	Google Chrome	Google Chron
chrome.ese	14772	TCP	99478	2800:98:110fa/L	443	https	2606:50±0:8001_		Established					C:(Program Files):Google):Chrome(Application):chrome	Google Chrome	Google Chron
chrome.ese	14772	TCP	99615	2800:98:110EaG.	48	https	2a044e42:3d:3		Established					C:\Program Files Google Chrome Application chrome	Google Chrome	Google Chron
chrome.exe	14772	TCP	60166	2800.98 1106.49.	48	https	2607/550-4006	mia09s16-in-x00.1	Established					C/\Program Files/iGoogle/Chrome/Application/chrome	Google Chrome	Google Chron
dirame.eve	14772	TCP	60597	2800/98/110ha/9.	5228		2607/f8b0i400c	uf-in-f188,1e100.net	Established					C/Program Files/Google/Chrome/Application/chrome	Google Chrome	Google Chron
chrome.eie	14772	TCP	62420	2800:98:110ha9.	48	https	2600 1403 8400	g2600-1403-8400	Established					C/\Program FilediGoogleiChrome\Applicationi.chrome	Google Chrome	Google Chron
chrome.eue	14772	UDP	5353					LAPTOP-GSMINLE.						C/Program Files/Google/Chrome/Application/chrome	Google Chrome	Google Chron
chrome.eve	25936	UDP	5353					LAPTOP-GSMNLE.						C/Program Files/Google/Chrome/Application/chrome	Google Chrome	Google Chron

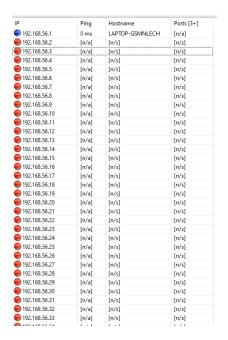
b. Identifique los puertos y las aplicaciones asociadas.

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	Discord.exe	21760	TCP	6463
chrome.exe	14772	TCP	60448	Discord.exe	24236	TCP	51115
chrome.exe	14772	UDP	5353	Discord.exe	24236	TCP	51117
chrome.exe	25936	UDP	5353	Discord.exe	24236	TCP	51129
chrome.exe	14772	TCP	49742	Discord.exe	24236	TCP	63037
chrome.exe	14772	TCP	59478	Discord.exe	24236	TCP	51120
chrome.exe	14772	TCP	59615	Discord.exe	24236	TCP	51121
chrome.exe	14772	TCP	60597	Discord.exe	21760	UDP	52528
chrome.exe	14772	UDP	5353	Discord.exe	24236	TCP	60218
chrome.exe	25936	UDP	5353	Discord.exe	21760	UDP	60435
© chrome.exe	14772	UDP	62725	Discord.exe	21760	UDP	57273
chrome.exe	14772	UDP	62725	Discord.exe	21700	UDP	31213
nvcontainer.ex	e 5284	UDP	10031				
nvcontainer.ex	e 28424	UDP	51549				
nvcontainer.ex	e 5012	UDP	55085				
nvcontainer.ex	e 5012	UDP	5353				
nvcontainer.ex	e 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		TCP	56276				
·— Cuál os la pri		.ı:£	-:			,	

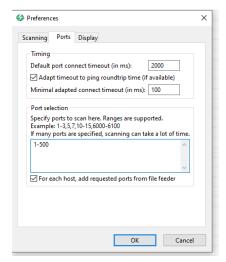
c. Cuál es la principal diferencia entre netstat y curports?

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. \

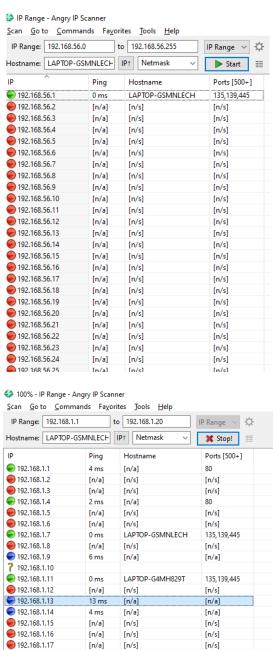
- 4. Ejecute el programa Angry IP Scanner
 - a. Haga un barrido de la red en la que se encuentra.



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







92.168.1.18

192.168.1.19

192.168.1.20

[n/a]

[n/a]

[n/s]

[n/s]

[n/s]

[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.