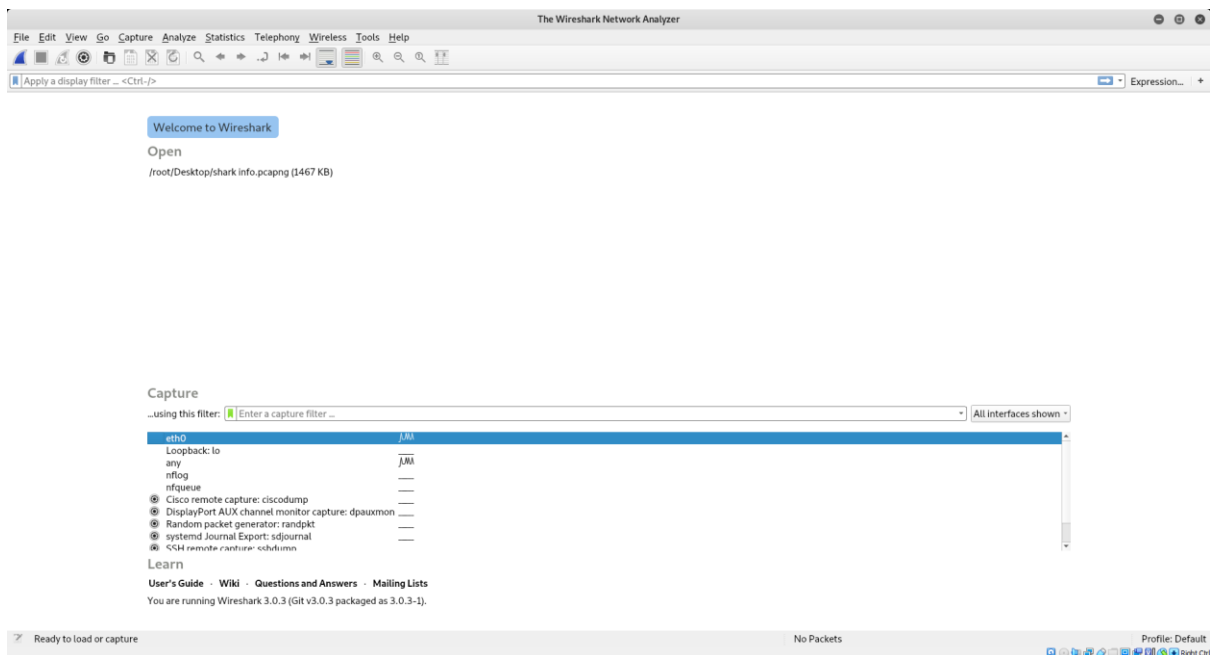


CYBER SECURITY OUTSTANDING PROJECTS

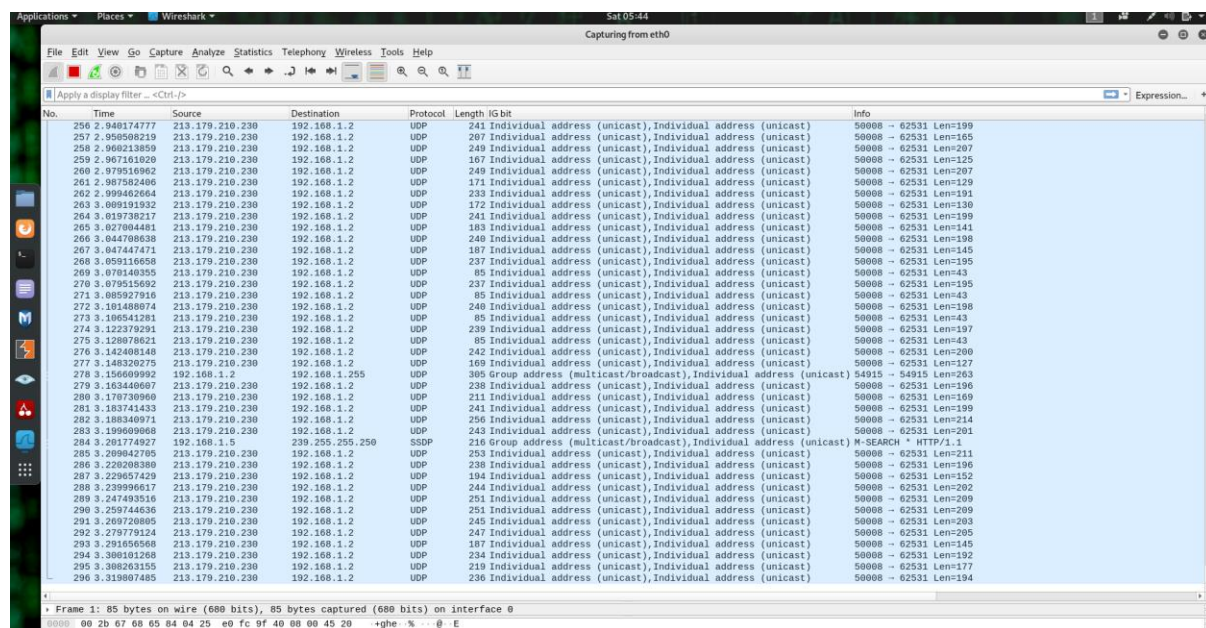
1. Use Wireshark to see traffic, in terms of source/destination IP address/ports, is going through your computer. Mention and document the traffic using snapshots that you see when all applications are closed, except background applications, in tabular form.

First download and install Wireshark in ur PC

Im using Kali Linux and I have installed Wireshark



Now start and run Wireshark and Scan using it



The image shows a Wireshark window titled "Capturing from eth0" with a display filter of "Apply a display filter... <Ctrl-F>". The packet list shows 296 captured packets, all of which are UDP packets from source 213.179.210.230 to destination 192.168.1.2. The packets are numbered 256 to 296. The packet details pane shows the structure of a UDP packet, including Ethernet II, Internet Protocol Version 4, and User Datagram Protocol. The packet bytes pane shows the raw data of the selected packet, which is 85 bytes long.

No.	Time	Source	Destination	Protocol	Length	IG bit	Info
256	2.948374777	213.179.210.230	192.168.1.2	UDP	241	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=199
257	2.950508219	213.179.210.230	192.168.1.2	UDP	207	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=165
258	2.960213859	213.179.210.230	192.168.1.2	UDP	249	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=207
259	2.967161020	213.179.210.230	192.168.1.2	UDP	167	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=125
260	2.979515962	213.179.210.230	192.168.1.2	UDP	249	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=207
261	2.987582406	213.179.210.230	192.168.1.2	UDP	171	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=129
262	2.999462664	213.179.210.230	192.168.1.2	UDP	233	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=191
263	3.009191932	213.179.210.230	192.168.1.2	UDP	172	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=130
264	3.019738217	213.179.210.230	192.168.1.2	UDP	241	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=199
265	3.027804481	213.179.210.230	192.168.1.2	UDP	183	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=141
266	3.044708638	213.179.210.230	192.168.1.2	UDP	248	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=198
267	3.047447471	213.179.210.230	192.168.1.2	UDP	187	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=145
268	3.059116658	213.179.210.230	192.168.1.2	UDP	237	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=195
269	3.070140355	213.179.210.230	192.168.1.2	UDP	85	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=43
270	3.079515602	213.179.210.230	192.168.1.2	UDP	237	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=195
271	3.085927916	213.179.210.230	192.168.1.2	UDP	85	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=43
272	3.101488074	213.179.210.230	192.168.1.2	UDP	248	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=198
273	3.106543281	213.179.210.230	192.168.1.2	UDP	85	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=43
274	3.122379291	213.179.210.230	192.168.1.2	UDP	238	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=197
275	3.128978621	213.179.210.230	192.168.1.2	UDP	85	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=43
276	3.142408148	213.179.210.230	192.168.1.2	UDP	242	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=200
277	3.148320275	213.179.210.230	192.168.1.2	UDP	169	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=127
278	3.156609992	192.168.1.2	192.168.1.255	UDP	305	Group address (multicast/broadcast), Individual address (unicast)	54915 -> 54915 Len=263
279	3.163440607	213.179.210.230	192.168.1.2	UDP	238	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=196
280	3.170739960	213.179.210.230	192.168.1.2	UDP	211	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=169
281	3.183741433	213.179.210.230	192.168.1.2	UDP	241	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=199
282	3.188340971	213.179.210.230	192.168.1.2	UDP	256	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=214
283	3.199690908	213.179.210.230	192.168.1.2	UDP	243	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=201
284	3.201774927	192.168.1.5	219.255.255.250	SSDP	216	Group address (multicast/broadcast), Individual address (unicast)	M-SEARCH * HTTP/1.1
285	3.209042705	213.179.210.230	192.168.1.2	UDP	253	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=211
286	3.220208380	213.179.210.230	192.168.1.2	UDP	238	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=196
287	3.229057429	213.179.210.230	192.168.1.2	UDP	194	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=152
288	3.239996617	213.179.210.230	192.168.1.2	UDP	244	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=202
289	3.247493516	213.179.210.230	192.168.1.2	UDP	251	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=209
290	3.259744536	213.179.210.230	192.168.1.2	UDP	251	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=209
291	3.269728805	213.179.210.230	192.168.1.2	UDP	245	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=203
292	3.279779124	213.179.210.230	192.168.1.2	UDP	247	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=205
293	3.291656568	213.179.210.230	192.168.1.2	UDP	187	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=145
294	3.306101268	213.179.210.230	192.168.1.2	UDP	234	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=192
295	3.308263155	213.179.210.230	192.168.1.2	UDP	219	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=177
296	3.319807485	213.179.210.230	192.168.1.2	UDP	236	Individual address (unicast), Individual address (unicast)	50008 -> 62531 Len=194

Even though all the background operations are closed there are many open ports going through the interface

Now we save and tabulate all the Traffic in the device with their port address.

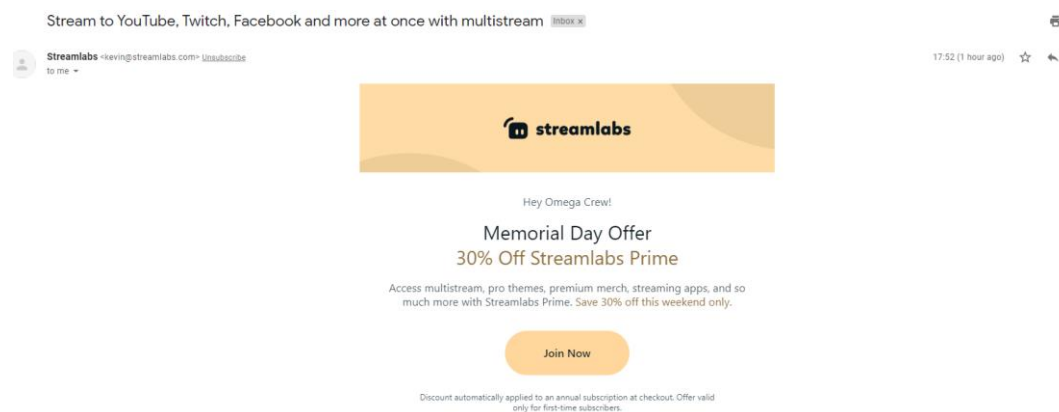
As there is more data in it I have attached it in the name of "ipv4.txt and ipv6.txt".

2. Use google apps toolbox to review email headers

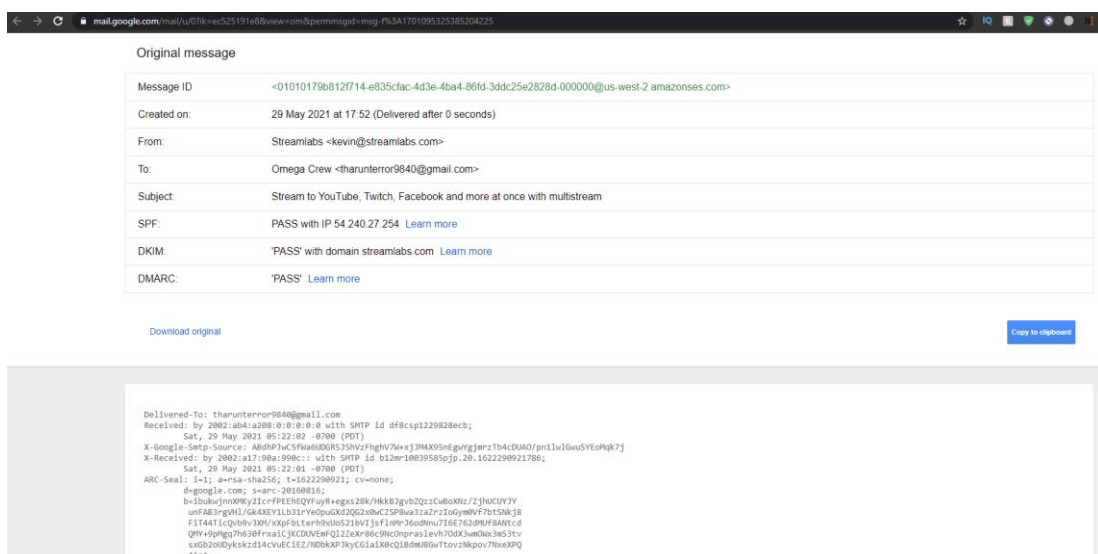
This method is used to find hackers who are relaying their messages through multiple server to make them untraceable.

Im am going to take a example mail from streamlabs.com to demonstrate this process.

First open the mail



Now right click on the mail settings and click “ show original “.



Now copy the email header and paste it in

<https://toolbox.googleapps.com/apps/messageheader/>

From this we can analyse the email routes and redirections and also the client and recipient .

Google Admin Toolbox Messageheader					Help
MessageId	01010179b8127714-e835cfac-4d3e-4ba4-86fd-3ddc25e2828d-000000@us-west-2.amazonaws.com				
Created at:	5/29/2021, 5:52:01 PM GMT+5:30 (Delivered after 1 sec)				
From:	Streamlabs <kevin@streamlabs.com>				
To:	Omega Crew <tharuntemor9840@gmail.com>				
Subject:	Stream to YouTube, Twitch, Facebook and more at once with multistream				
SPF:	pass with IP 54.240.27.254 Learn more				
DKIM:	pass with domain streamlabs.com pass with domain amazonses.com Learn more				
DMARC:	pass Learn more				
#	Delay	From *	To *	Protocol	Time received
0		a27-254.smtp-out-us-west-2.amazonaws.com.	→ [Google] mx.google.com	ESMTPS	5/29/2021, 5:52:01 PM GMT+5:30
1			→ [Google] 2002:a17:90a:990c::	SMTP	5/29/2021, 5:52:01 PM GMT+5:30
2	1 sec		→ [Google] 2002:ab4:a208:0:0:0:0:0	SMTP	5/29/2021, 5:52:02 PM GMT+5:30

3. Download “Nessus Professional” software tool (A Port Scanner) from the

link <https://www.tenable.com/> and install in your system.

You can

sign-in for a free trail and down load for your laptop or desktop OS

compatible version. Install in your computer and use the configuration

user guide and configure:

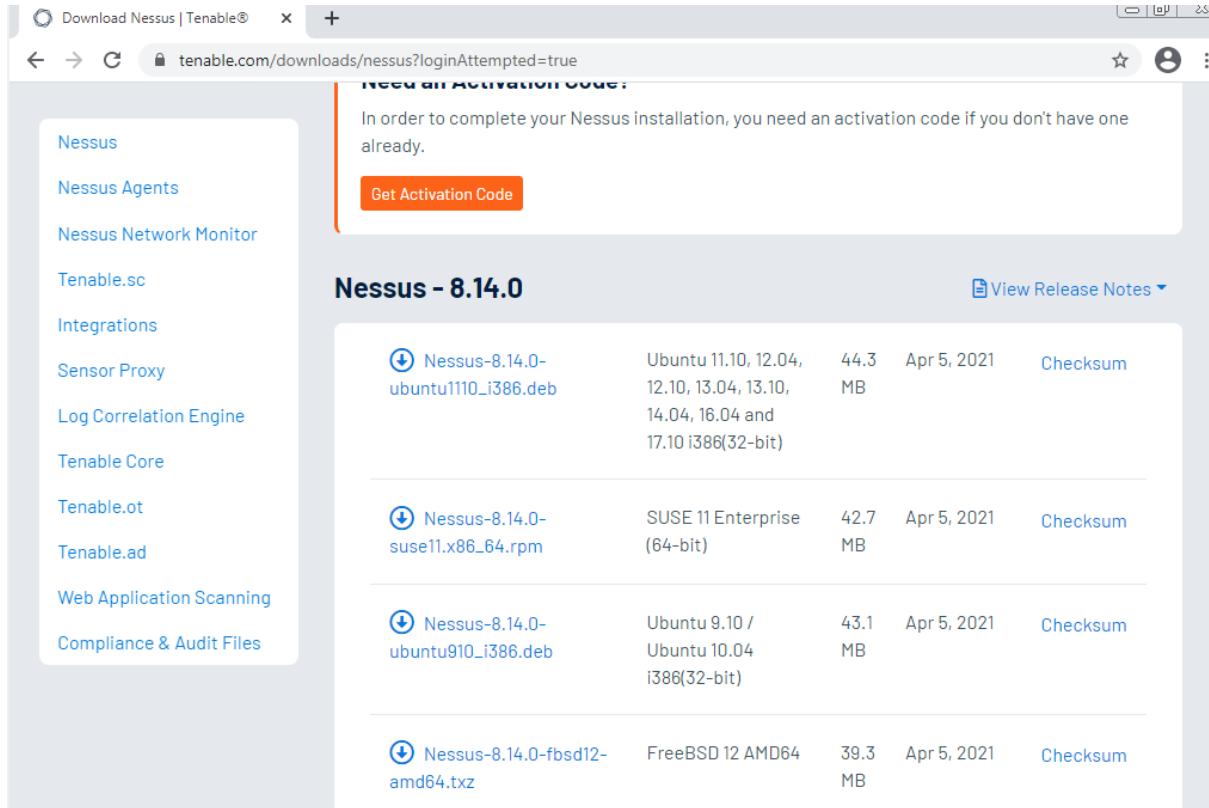
a. Use Nessus tool and scan your entire OS and identify what are all the ports that are open.

b. List at least 10 applications and the corresponding ports used by

them.

c. List the Network Protocol that each of the applications uses.

First register your details in www.tenable.com and download the setup



Download Nessus | Tenable®

tenable.com/downloads/nessus?loginAttempted=true

Need an Activation Code:

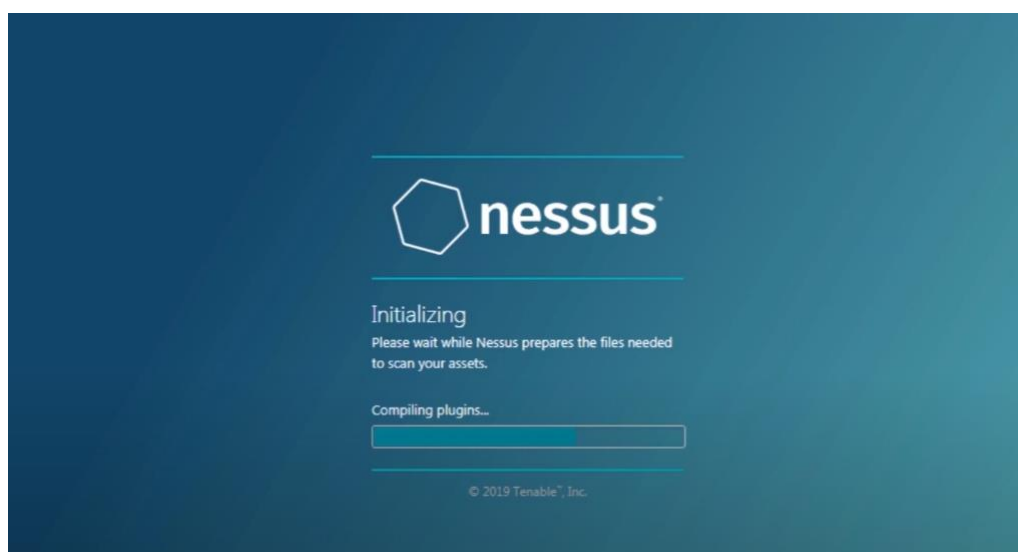
In order to complete your Nessus installation, you need an activation code if you don't have one already.

[Get Activation Code](#)

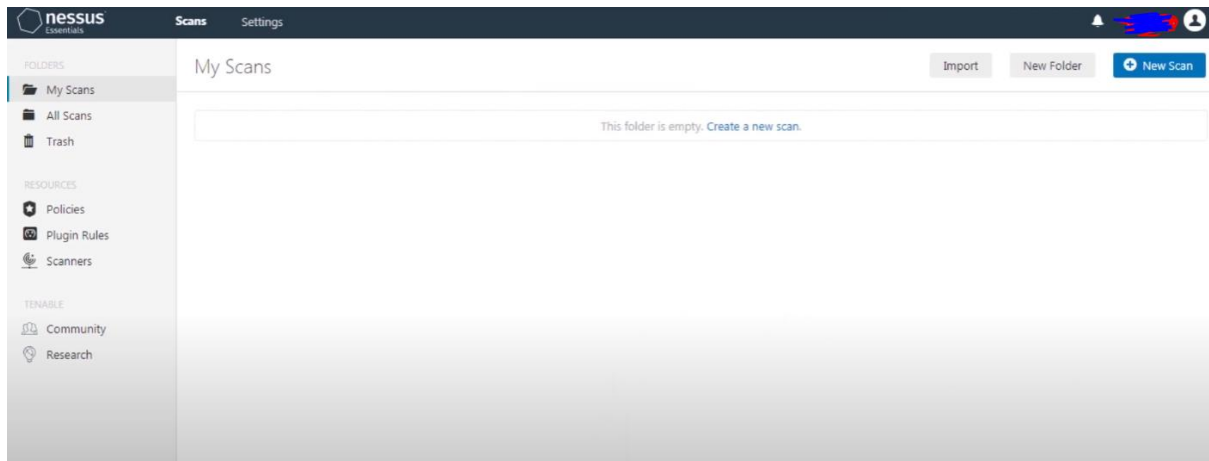
Nessus - 8.14.0 [View Release Notes](#)

Nessus-8.14.0-ubuntu1110_i386.deb	Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 16.04 and 17.10 i386(32-bit)	44.3 MB	Apr 5, 2021	Checksum
Nessus-8.14.0-suse11.x86_64.rpm	SUSE 11 Enterprise (64-bit)	42.7 MB	Apr 5, 2021	Checksum
Nessus-8.14.0-ubuntu910_i386.deb	Ubuntu 9.10 / Ubuntu 10.04 i386(32-bit)	43.1 MB	Apr 5, 2021	Checksum
Nessus-8.14.0-fbsd12-amd64.txz	FreeBSD 12 AMD64	39.3 MB	Apr 5, 2021	Checksum

After installing the software will auto direct to a local host port where the software will further download and install

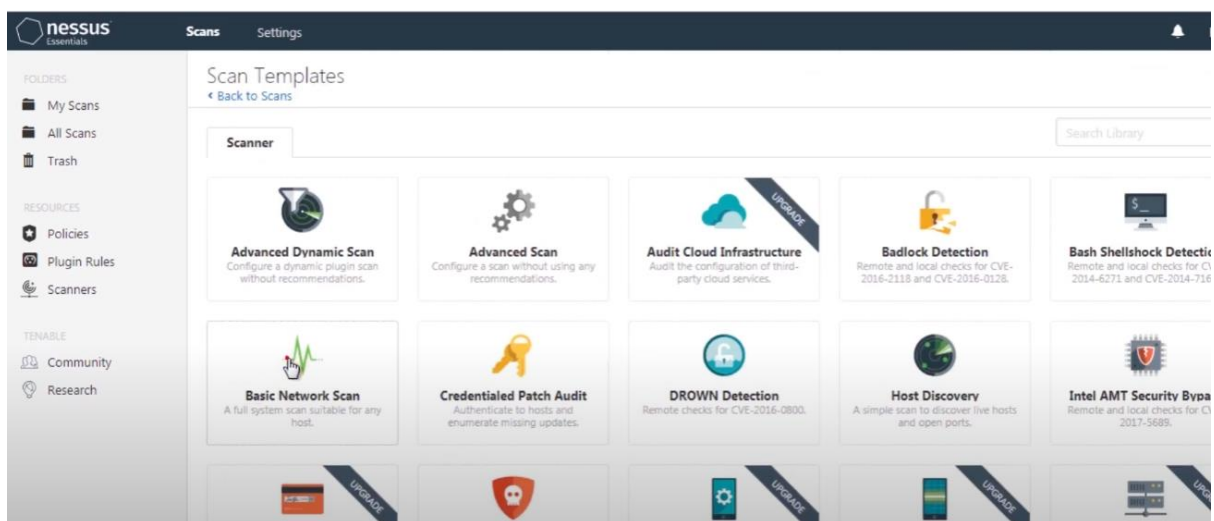


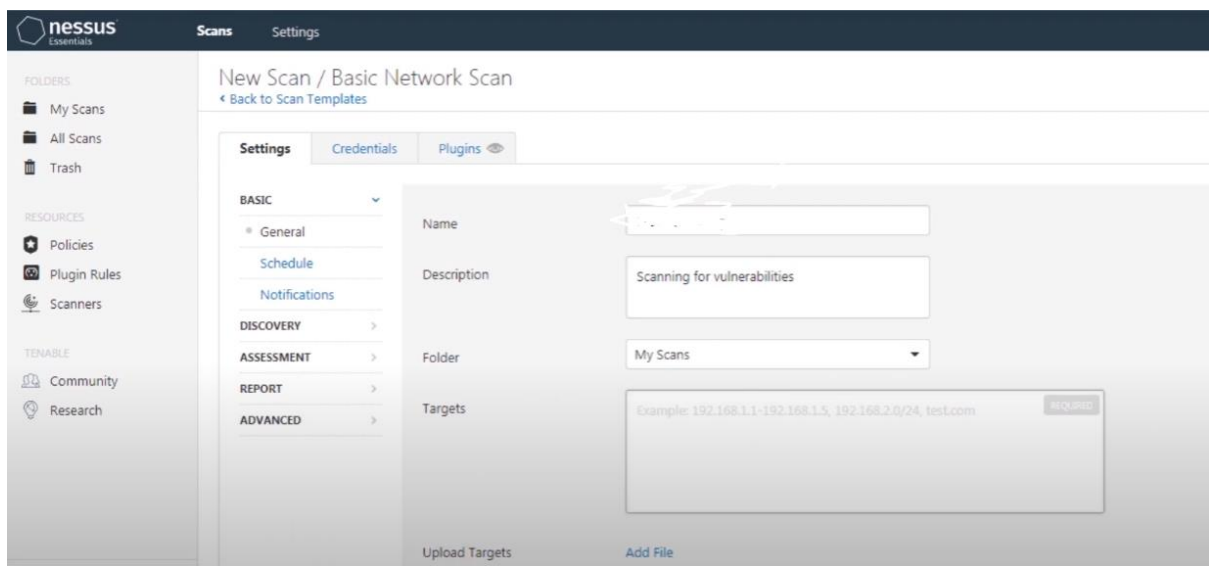
After installing this Nessus scan page will open where we can see all our scans



Now I am going to scan the network using basic scan to get the details of the currently running applications with their ports.

Some of the open ports which are available for listening are 4720, 1144, 8812, 4 and so on





Now I fill my info and the target is my ip address as I am going to scan my own pc.

After this can I can get all the vulnerabilities and the applications which are running in my computer

Some of the applications are :

<u>Application</u>	<u>port</u>	<u>network protocol</u>
Windows	53	TCP,UDP
Discord	443	TCP
Spotify	4070	TCP
Steam	80	TCP
Steampow.	443	HTTPS
Chrome	9100	TCP,HTTPS
Microsoft365	3478	TCP
Ubisoft store	6667	UDP
Nvidia	35043	TCP
Qbittorrent	49172	TCP
OracleVM	7002	TCP

