Cyber Security Major Project

Network Traffic Analysis Tool

Name- Ketaki Deo

Email ID – ketaki.deo03@gmail.com

The project has been made using Python and various Python libraries like tkinter, snapy, etc. to make the gui and analyse traffic.

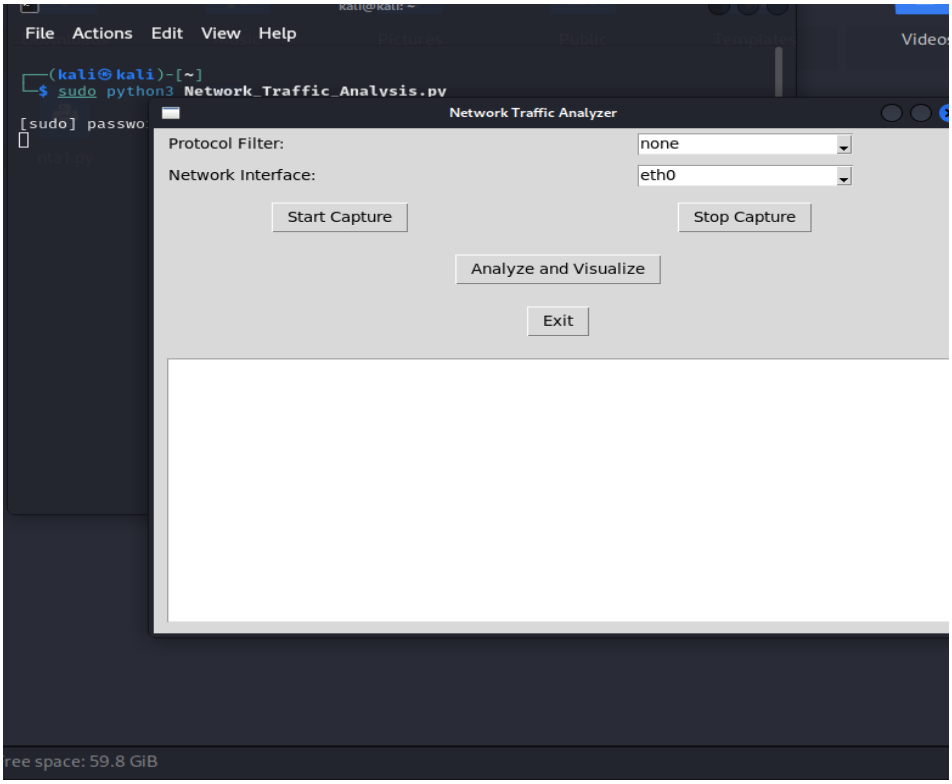
Steps to run the program –

1. Open the terminal in kali Linux.

2. Type “sudo python3 Network_Traffic_Analysis.py”.

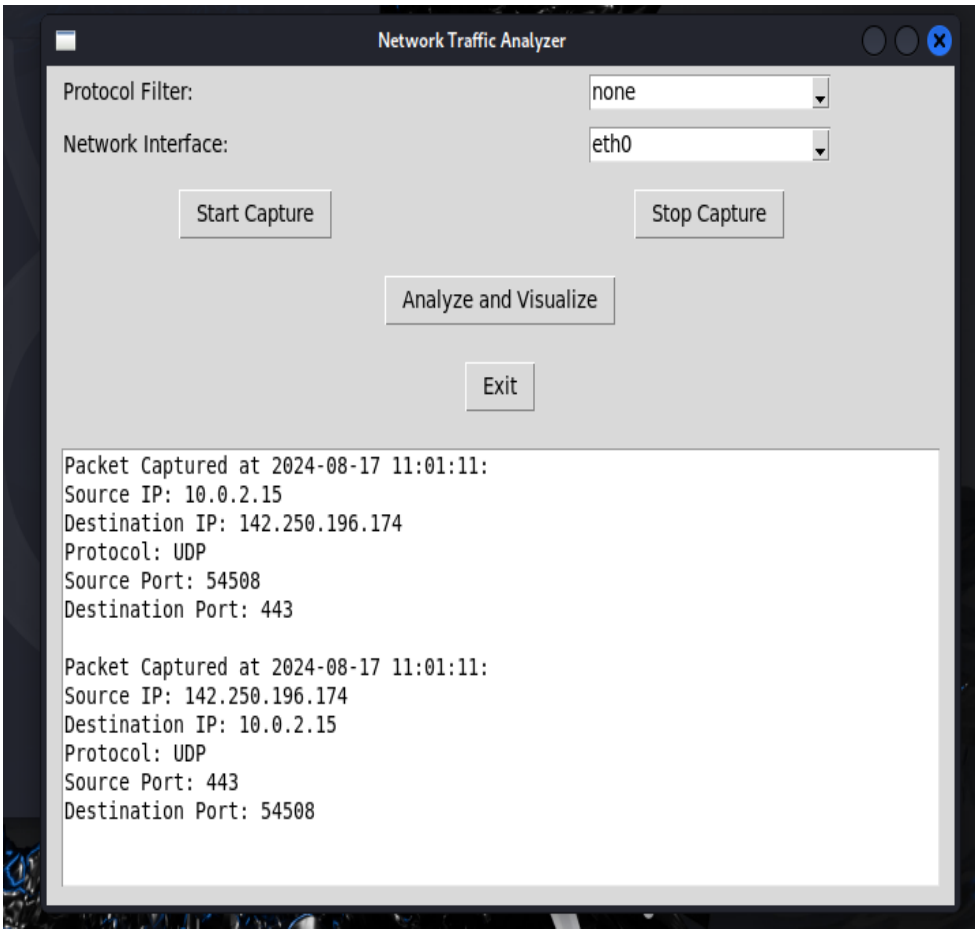
3. It will ask for password, enter the password and hit enter.

4. A window will appear as such:



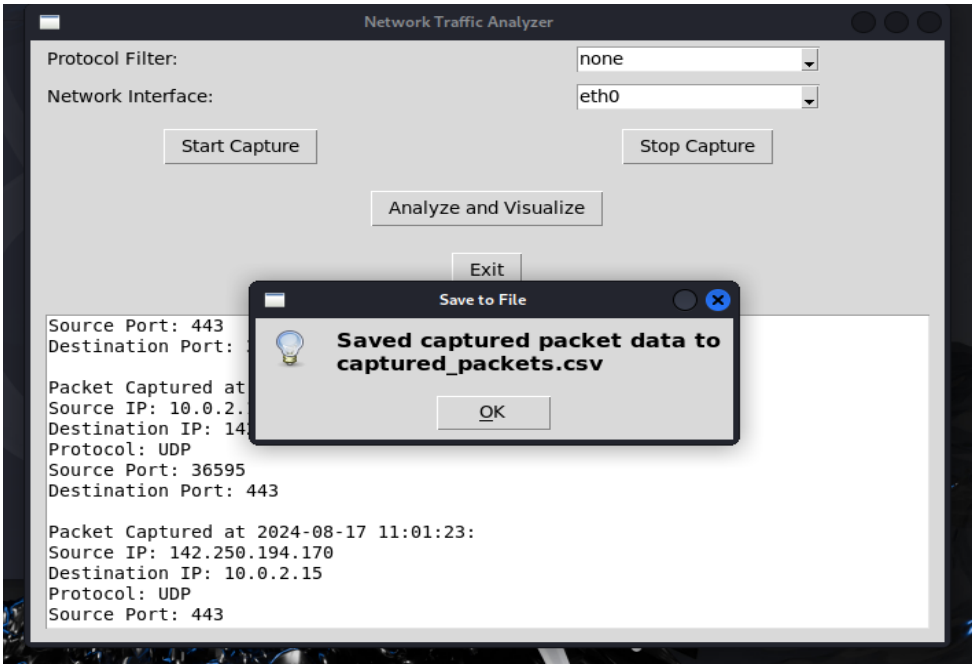
5. Select the required filters and click on the “Start Capture” button.

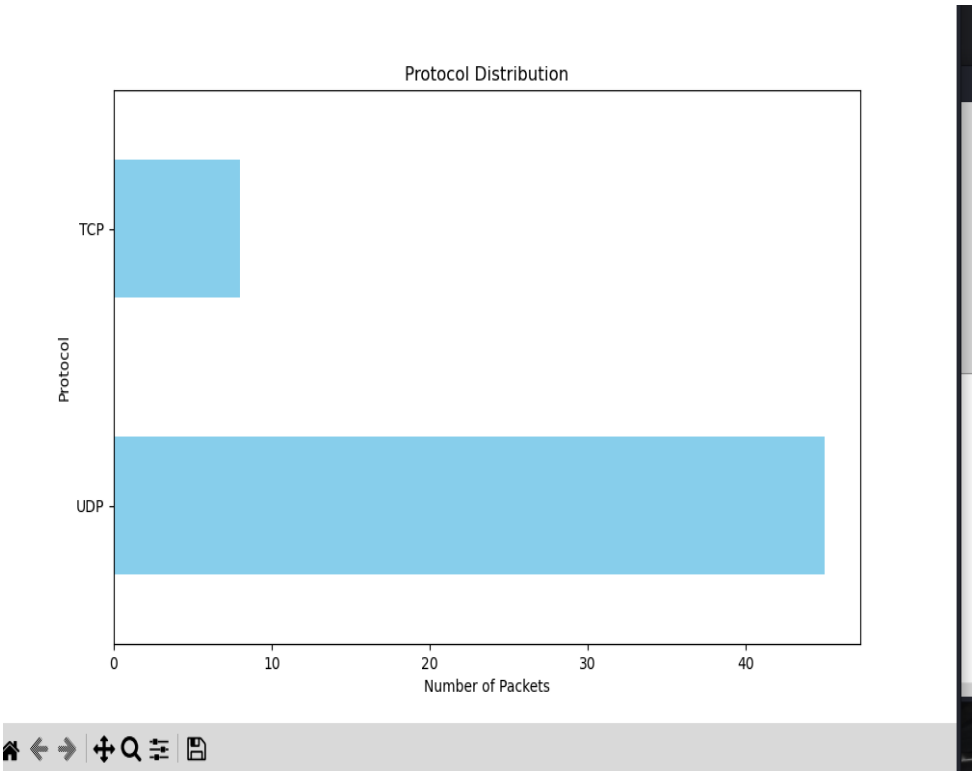
6. It will start capturing the packets.

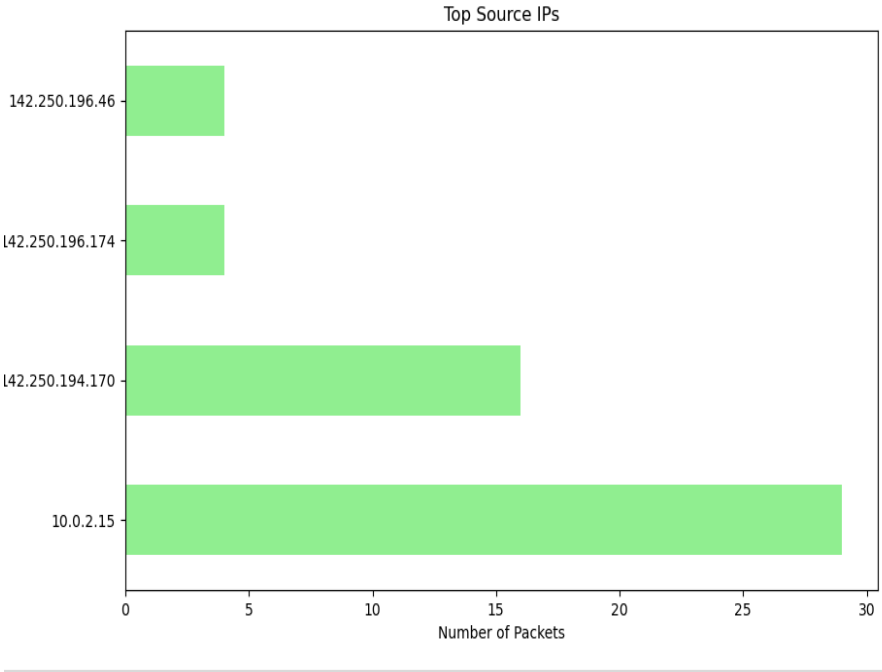


7. After you are done capturing click on the “Stop Capture” button.

8. “Analyse and visualise” button will give you a graph of the analysis of the captured packet data and save the output in a csv file called “captured_packets”.


Network Traffic Analyzer
Protocol Filter:
none
Network Interface:
eth0
Start Capture
Stop Capture
Analyze and Visualize
Exit
Save to File
Saved captured packet data to captured_packets.csv
OK
Source Port: 443
Destination Port:
Packet Captured at
Source IP: 10.0.2.
Destination IP:
Protocol: UDP
Source Port: 36595
Destination Port: 443
Packet Captured at 2024-08-17 11:01:23:
Source IP: 142.250.194.170
Destination IP: 10.0.2.15
Protocol: UDP
Source Port: 443


Protocol Distribution
TCP
UDP
Protocol
0
10
20
30
40
Number of Packets



~/captured_packets.csv [Read Only] - Mousepad

File Edit Search View Document Help

```
1 Timestamp,Source IP,Destination IP,Protocol,Source Port,Destination Port,Malicious
2 2024-08-17 11:01:30,142.250.194.170,10.0.2.15,UDP,443,36595,0
3 2024-08-17 11:01:30,142.250.194.170,10.0.2.15,UDP,443,36595,0
4 2024-08-17 11:01:30,10.0.2.15,142.250.194.170,UDP,36595,443,1
5 2024-08-17 11:01:30,10.0.2.15,142.250.194.170,UDP,36595,443,1
6 2024-08-17 11:01:30,142.250.194.170,10.0.2.15,UDP,443,36595,0
7 2024-08-17 11:01:30,10.0.2.15,142.250.194.170,UDP,36595,443,1
8 2024-08-17 11:01:30,142.250.194.170,10.0.2.15,UDP,443,36595,0
9 2024-08-17 11:01:30,10.0.2.15,142.250.194.170,UDP,36595,443,1
10 2024-08-17 11:01:30,142.250.194.170,10.0.2.15,UDP,443,36595,0
11 2024-08-17 11:01:30,10.0.2.15,142.250.194.170,UDP,36595,443,1
12 2024-08-17 11:01:30,10.0.2.15,142.250.194.170,UDP,36595,443,1
13 2024-08-17 11:01:30,10.0.2.15,142.250.194.170,UDP,36595,443,1
14 2024-08-17 11:01:30,142.250.194.170,10.0.2.15,UDP,443,36595,0
15 2024-08-17 11:01:30,10.0.2.15,142.250.194.170,UDP,36595,443,1
16 2024-08-17 11:01:30,142.250.194.170,10.0.2.15,UDP,443,36595,0
17 2024-08-17 11:01:30,10.0.2.15,142.250.194.170,UDP,36595,443,1
18 2024-08-17 11:01:30,10.0.2.15,142.250.194.170,UDP,36595,443,1
19 2024-08-17 11:01:30,142.250.194.170,10.0.2.15,UDP,443,36595,0
20 2024-08-17 11:01:30,10.0.2.15,142.250.196.174,UDP,54508,443,1
21 2024-08-17 11:01:30,10.0.2.15,142.250.196.174,UDP,54508,443,1
22 2024-08-17 11:01:30,10.0.2.15,142.250.196.174,UDP,54508,443,1
23 2024-08-17 11:01:30,10.0.2.15,142.250.196.174,UDP,54508,443,1
24 2024-08-17 11:01:30,142.250.196.174,10.0.2.15,UDP,443,54508,0
25 2024-08-17 11:01:30,10.0.2.15,142.250.196.174,UDP,54508,443,1
26 2024-08-17 11:01:30,142.250.196.174,10.0.2.15,UDP,443,54508,0
27 2024-08-17 11:01:30,10.0.2.15,142.250.196.174,UDP,54508,443,1
28 2024-08-17 11:01:30,142.250.196.174,10.0.2.15,UDP,443,54508,0
29 2024-08-17 11:01:30,10.0.2.15,142.250.196.174,UDP,54508,443,1
30 2024-08-17 11:01:30,142.250.196.174,10.0.2.15,UDP,443,54508,0
31 2024-08-17 11:01:30,10.0.2.15,142.250.196.46,TCP,57674,443,1
32 2024-08-17 11:01:30,142.250.196.46,10.0.2.15,TCP,443,57674,0
```

9. Exit button will exit the analyser.

Thank you!