Packet Analyzer

Created an essential tool for monitoring, analyzing, and troubleshooting networks. It has capabilities such as packet capturing, protocol analysis, and traffic monitoring.

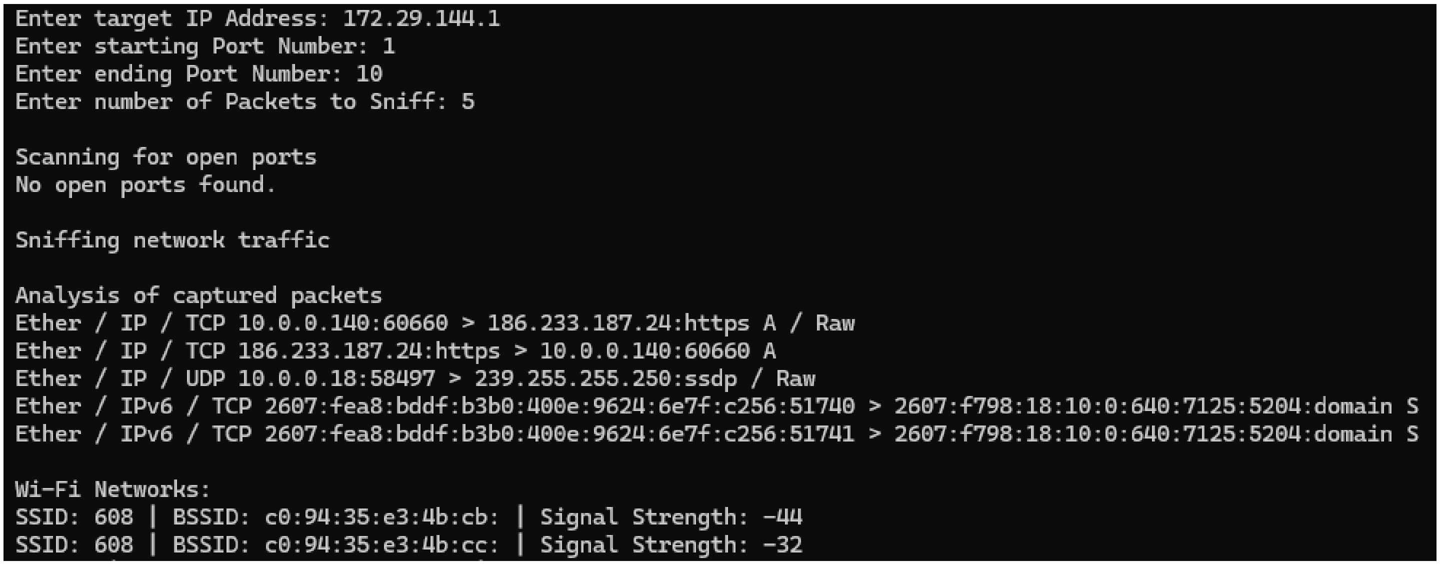
This project was created to understand the concepts of networking such as sockets, packet sniffing and the way we can interact with network devices and protocols.

It has the following features:

- Port Scanning: It scans a range of TCP ports on a specified target IP address to determine which ports are open and available for communication. This can be useful for identifying potential entry points for network attacks or vulnerabilities.
- Packet Sniffing: It captures a specified number of network packets on the specified network interface. Packet sniffing allows you to inspect the data flowing through the network, which can be helpful for troubleshooting network issues or analyzing network traffic for security purposes.
- Wi-Fi Network Analysis: It scans for nearby Wi-Fi networks and displays information about them, including their SSID, BSSID (MAC address), and signal strength. This functionality can be useful for monitoring Wi-Fi networks in the vicinity or troubleshooting Wi-Fi connectivity problems.

So, the code will ask for the Target IP address, starting port number to ending, and the number of packets to sniff. Once the user enters it, we see the output shown in the screenshot.

Below screenshot represents the sample output:



```
Enter target IP Address: 172.29.144.1
Enter starting Port Number: 1
Enter ending Port Number: 10
Enter number of Packets to Sniff: 5

Scanning for open ports
No open ports found.

Sniffing network traffic

Analysis of captured packets
Ether / IP / TCP 10.0.0.140:60660 > 186.233.187.24:https A / Raw
Ether / IP / TCP 186.233.187.24:https > 10.0.0.140:60660 A
Ether / IP / UDP 10.0.0.18:58497 > 239.255.255.250:ssdp / Raw
Ether / IPv6 / TCP 2607:fea8:bddf:b3b0:400e:9624:6e7f:c256:51740 > 2607:f798:18:10:0:640:7125:5204:domain S
Ether / IPv6 / TCP 2607:fea8:bddf:b3b0:400e:9624:6e7f:c256:51741 > 2607:f798:18:10:0:640:7125:5204:domain S

Wi-Fi Networks:
SSID: 608 | BSSID: c0:94:35:e3:4b:cb: | Signal Strength: -44
SSID: 608 | BSSID: c0:94:35:e3:4b:cc: | Signal Strength: -32
```

Analysis of the captured packets:

- The ‘sniff’ function from Scapy is used to capture network packets.
  - **Eg: “Ether / IP / TCP 10.0.0.140:60660 > 186.233.187.24:https A / Raw”**
  - "Ether" refers to the Ethernet frame header, which contains information like source and destination MAC addresses.
  - "IP" means the Internet Protocol, which handles addressing and routing of packets across a network.
  - "TCP" refers to the Transmission Control Protocol, which provides reliable, connection-oriented communication between devices.
  - "UDP" refers to the User Datagram Protocol, which provides connectionless communication with minimal overhead.
  - "IPv6" refers to Internet Protocol version 6, an updated version of IPv4 with larger address space and other improvements.
  - The first IP address and port number represent the source of the packet.
  - The second IP address and port number represent the destination of the packet.
  - The payload after the protocol headers (e.g., "https", "ssdp", "domain") represents the application-layer protocol being used (e.g., HTTPS, SSDP, DNS).

Analysis of the result in Wi-Fi networks:

- **Eg: SSID: 608 | BSSID: c0:94:35:e3:4b:cb: | Signal Strength: -44**
- “SSID": This stands for Service Set Identifier, which is the name of the Wi-Fi network. In this case, the SSID is "608".
- "BSSID": This stands for Basic Service Set Identifier, which is the MAC address of the access point (router) that hosts the Wi-Fi network. In this case, the BSSID is "c0:94:35:e3:4b:cb".
- "Signal Strength": This indicates the signal strength of the Wi-Fi network, typically measured in dBm (decibels relative to one milliwatt). A higher value (less negative) indicates a stronger signal. In this case, the signal strength is "-44" dBm.

Link to code: https://github.com/jay-patel-07/Packet_Analyzer