### **TASK 1**

### **Basic Network Sniffer**

### **Installation**

First, you'll need to install scapy:

| pip install scapy |
| --- |

### **Code**

Here's a basic implementation of a network sniffer using scapy:

| **from** scapy.all **import** \*  **def** **packet\_callback**(packet):  **if** IP **in** packet:  src\_ip = packet[IP].src  dst\_ip = packet[IP].dst  protocol = packet[IP].proto    **if** protocol == 6 **and** TCP **in** packet: # TCP  src\_port = packet[TCP].sport  dst\_port = packet[TCP].dport  print(f'TCP Packet: {src\_ip}:{src\_port} --> {dst\_ip}:{dst\_port}')   **elif** protocol == 17 **and** UDP **in** packet: # UDP  src\_port = packet[UDP].sport  dst\_port = packet[UDP].dport  print(f'UDP Packet: {src\_ip}:{src\_port} --> {dst\_ip}:{dst\_port}')   **elif** protocol == 1 **and** ICMP **in** packet: # ICMP  icmp\_type = packet[ICMP].type  icmp\_code = packet[ICMP].code  print(f'ICMP Packet: {src\_ip} --> {dst\_ip} Type: {icmp\_type} Code: {icmp\_code}')  **def** **start\_sniffing**():  sniff(prn=packet\_callback, store=**False**)  **if** \_\_name\_\_ == '\_\_main\_\_':  start\_sniffing() |
| --- |

**Explanation**

1. **Imports**:

* from scapy.all import \*: Importing all functions and classes from scapy, which is used for constructing and dissecting network packets.

1. **packet\_callback(packet)**:

* This function is called for each packet captured by sniff().
* It checks if the packet is an IP packet (IP in packet).
* Depending on the protocol (TCP, UDP, ICMP), it extracts and prints relevant information such as source IP, destination IP, source port, destination port, ICMP type, and ICMP code.

1. **start\_sniffing()**:

* This function starts capturing packets using sniff() from scapy.
* prn=packet\_callback specifies the callback function to be called for each captured packet.
* store=False ensures that captured packets are not stored in memory to avoid running out of memory when capturing for long periods.

1. **Main section**:

* start\_sniffing() is called to begin capturing and analyzing network traffic.

### **Usage**

* Run the script with root/administrator privileges to capture network traffic:

| sudo python sniffer.py |
| --- |

### **Notes**

* This is a basic example. Scapy allows for extensive packet manipulation and analysis, including crafting and sending packets.
* Ensure to run this script responsibly and in compliance with applicable laws and regulations.
* For more advanced features or specific protocol handling, you may need to extend the script further.