Ex.No:11

Practical - 11

Aim:

To implement packet sniffing using RAW sockets.

Algorithm:

* Check for root privileges & open a new socket bound to chosen network interface.
* Receive raw frames from socket (recvfrom) in a loop.
* Parse Ethernet header to extract source MAC, Destination MAC, Ether Type.
* If Ether Type == IPv4, Parse the IPv4 header to get version, IHL, TTL, Protocol, source IP, Destination IP and Payload.
* Print the summary
* Repeat until stopped, then close socket & Exit cleanly.

Code:

```
def Packet_callback(Packet):
    if IP in Packet:
        ip_layer = Packet[IP]
        Protocol = ip_layer.Proto
        src_ip = ip_layer.src
        dst_ip = ip_layer.dst
        Protocol_name = ""
        if Protocol == 1:
            Protocol_name = "ICMP"
        elif Protocol == 6:
            Protocol_name = "TCP"
        elif Protocol == 17:
            Protocol_name = "UDP"
        else:
            Protocol_name = "Unknown Protocol"
        Print(f"Protocol: {Protocol_name}")
        Print(f"source IP: {src_ip}")
        Print(f"Destination IP: {dst_ip}")
        Print("-" * 30)
    sniff(face = 'WIFI', Prn = Packet_callback,
          filter = 'ip', store = 0)
```

Input:

Pinging a server (ping)

Output:

Protocol : TCP

Source IP : 192.168.1.5

Destination IP : 172.217.15.78

- - - - - - - - -

Protocol : ICMP

Source IP : 192.168.1.5

Destination IP : 8.8.8.8

- - - - - - - - - -

Protocol : UDP

Source IP : 192.168.1.5

Destination IP : 224.0.0.251

Result:

Packet sniffing using Raw sockets is implemented & Executed.