EX.NO: 4

23/7/25

IMPLEMENT PACKET SNIFFING USING RALI SOCKETS IN PYTHON.

AIM:

To capture and display packet details (source, MAC, destination, payload) using python will slapy on windows.

ALGORITHM:

1. It up the necessary imports from the scapy library.

2. Define a function to handle the capture packets extracting and painting the relevant information.

3. ~~Call~~ Print a message to indicate that the script is listening for a packet.

4. Call the sniff function from scapy. passing the packet-call back function.

5. The script will capture a single packet ar process it using packet-call back function.

CODE:

```
from scapy.all import sniff Ether
def packet-callback (packet):
    if Ether in packet:
        ether: packet [Ether]
        print( f" source MAC: { ether.src}")
        print( f" Destination MAC: { ether.dst}")
        print ( f "Payload : { bytes (packet.
                    payload ) - hex ()[:100]}")
        print ( " -"*60)
```

```
print ("Listing for a packet .... (press ctrl+c to stop)")
sniff (prn = packet_callback, count=1).
```

RESULT

Thus a single packet is sniffed & source, destination MA are displayed with payload in windows.

OUTPUT:

Source MAC: 3c 15 : c2 16 : 5b : d : 20

DESTINATION MAC : ff : ff : ff : ff : ff

Payload : 08004500002 8d431400640116861160801 80404