Roll No: 241901095

Name:Sakthivel M

Department: CSE-Cyber Security

IMPLEMENT PACKET SNIFFING USING RAW SOCKETS IN PYTHON

AIM:

To capture and inspect network packets on a local interface using Python raw sockets — for learning or authorized troubleshooting (show source/destination MAC/IP, protocol, and ports).

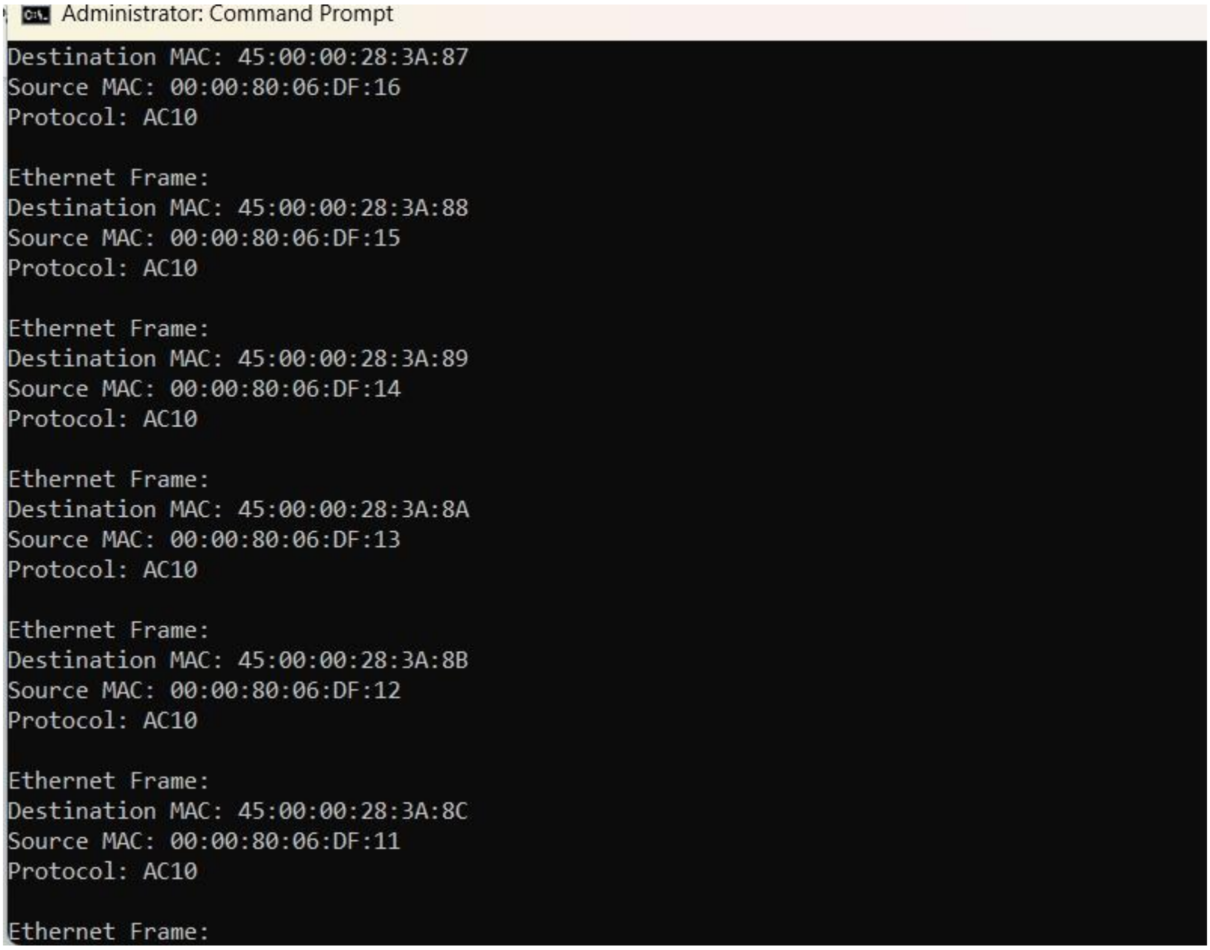
PROCEDURE:

1. Confirm you have permission to sniff the target network.
2. Open a raw socket at the link layer (AF_PACKET, SOCK_RAW) to receive frames.
3. Bind the socket to the interface you want to monitor (e.g., eth0).
4. Loop reading packets from the socket.
5. Parse minimal headers (Ethernet → IPv4 → TCP/UDP) to extract addresses/ports.
6. Print/store/analyze the fields you care about.
7. Close the socket and stop when finished.

PROGRAM:

```
 import socket

import struct

import binascii

import textwrap


def main():
    host = socket.gethostbyname(socket.gethostname())
    print('IP: {}'.format(host))

    conn = socket.socket(socket.AF_INET, socket.SOCK_RAW, socket.IPPROTO_IP)
    conn.bind((host, 0))

    conn.setsockopt(socket.IPPROTO_IP, socket.IP_HDRINCL, 1)

    conn.ioctl(socket.SIO_RCVALL, socket.RCVALL_ON)

    while True:
        raw_data, addr = conn.recvfrom(65536)

        dest_mac, src_mac, eth_proto, data = ethernet_frame(raw_data)

        print('\nEthernet Frame:')
        print("Destination MAC: {}".format(dest_mac))
        print("Source MAC: {}".format(src_mac))
        print("Protocol: {}".format(eth_proto))

def ethernet_frame(data):
    dest_mac, src_mac, proto = struct.unpack('!6s6s2s', data[:14])
    return get_mac_addr(dest_mac), get_mac_addr(src_mac),
get_protocol(proto), data[14:]

def get_mac_addr(bytes_addr):
    bytes_str = map('{:02x}'.format, bytes_addr)
    mac_address = ':'.join(bytes_str).upper()

    return mac_address


def get_protocol(bytes_proto):

    bytes_str = map('{:02x}'.format, bytes_proto)

    protocol = ''.join(bytes_str).upper()

    return protocol

main()
```

OUTPUT:



Administrator: Command Prompt

```
Destination MAC: 45:00:00:28:3A:87
Source MAC: 00:00:80:06:DF:16
Protocol: AC10

Ethernet Frame:
Destination MAC: 45:00:00:28:3A:88
Source MAC: 00:00:80:06:DF:15
Protocol: AC10

Ethernet Frame:
Destination MAC: 45:00:00:28:3A:89
Source MAC: 00:00:80:06:DF:14
Protocol: AC10

Ethernet Frame:
Destination MAC: 45:00:00:28:3A:8A
Source MAC: 00:00:80:06:DF:13
Protocol: AC10

Ethernet Frame:
Destination MAC: 45:00:00:28:3A:8B
Source MAC: 00:00:80:06:DF:12
Protocol: AC10

Ethernet Frame:
Destination MAC: 45:00:00:28:3A:8C
Source MAC: 00:00:80:06:DF:11
Protocol: AC10

Ethernet Frame:
```

RESULT:

The program shows the source and destination MAC address and protocol of network packets it captures.