Part B

5. Create a Python script that sends periodic UDP broadcast messages from one VM and another script that receives and displays them on a second VM. Capture this broadcast traffic in Wireshark and identify the broadcast MAC and IP addresses.

Step1 : Kali linux vm send a UDP broadcast message

```
import socket
import time
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
sock.setsockopt(socket.SOL_SOCKET, socket.SO_BROADCAST, 1)
for i in range(5):
    msg = "DEVICE_DISCOVERY_{}".format(i).encode()
    sock.sendto(msg, ("255.255.255.255", 4000))
    print("[Sent]", msg)
    time.sleep(1)
```

Step 2: ubuntu vm Listen for broadcast traffic

```
import socket
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
sock.bind(("", 4000))
print("Listening for broadcast packets...")
try:
    while True:
            data, addr = sock.recvfrom(1024)
             print(f"Broadcast from {addr}: {data.decode()}")
except KeyboardInterrupt:
             print(“Listener Stopped Manually”)
```

finally:

    sock.close()

Step 3: open Wireshark in Kali linux and Analyze the packets

udp.port == 4000

Step4:

In ubuntu vm before executing the python code, use below commands to allow udp packets

sudo ufw allow 4000/udp

sudo ufw status

sudo ufw reload

Step 5:

Then execute the python code in ubuntu

python3 broadcast_listener.py

Then execute the python code in kali linux vm

python broadcast_sender.py

Step 6:

Now observe the udp packets from kali linux to ubuntu(broadcast packets) by using filter

udp.port==4000

Step 7: Analyze

UDP packets sent from source: <kali linux ip> to Destination<broadcast-ip> i.e 255.255.255.255