3. Initiate an SSH session between two local systems or virtual machines. Capture traffic using Wireshark and analyse the session key exchange, encryption setup, and user authentication.

REQUIREMENTS:

- ✓ Two systems on the same local network or host-only VM network
  Example: VM1 (client), VM2 (server)
- ✓ OpenSSH installed
- ✓ Wireshark installed on either:
  the client machine, or
  the server machine, or
  a third machine capturing traffic (optional)

Step 1: Prepare the offline network

- ✓ We need machines to communicate locally without internet.

- ✓ Configure your two VMs: Kali Linux and Metasploitable2
  Example network:
- ✓ VM1-Kali Linux (client): <Kali Linux IP>
- ✓ VM2- Metasploitable2(server): <Metasploitable2 IP>
- ✓ Check both VM IP using ifconfig command.

Step 2: Enable SSH Service on Server Machine i.e on metasploitable2

- ✓ **Start the ssh service using below command**
  sudo /etc/init.d/ssh start

- ✓ **Check Listening port using**
  netstat -tlnp | grep 22

- ✓ **You will see below output**
  tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN

Step 3: Start Wireshark on Kali Linux

We will capture traffic from the client side (Kali).

- ✓ **Open Wireshark**
- ✓ **Select interface:**

  Usually eth0

  It will start capturing packets

Step 4: From Kali Initiate SSH Connection to Metasploitable2

- ✓ **Run the below command in Kali Linux Terminal**

```
ssh -o HostKeyAlgorithms=+ssh-rsa msfadmin@192.168.1.5
```

- ✓ **It will prompt you to enter the password. Then enter the password.**

Now you are inside the metasploitable2 Virtual Machine (Means you are able to access the Metasploitable2 VM from Kali Linux through SSH Connection)

- ✓ **Run the below commands to generate encrypted traffic**

  hostname
  ls
  id
  whoami

uname –a

✓ **Then Exit**

Exit

Step 5: Stop Wireshark and Analyze the SSH packets captured in Wireshark

✓ **Apply Filter**

tcp.port==22

✓ **You should below packets such as**

- tcp 3 way handshaking packets(Syn, Syn+Ack, Ack)
- Client Protocol, Server protocol
- Key Exchange Init
- Diffie Hellman Group Exchange
- Encrypted Packets…

Expand all the packets