

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

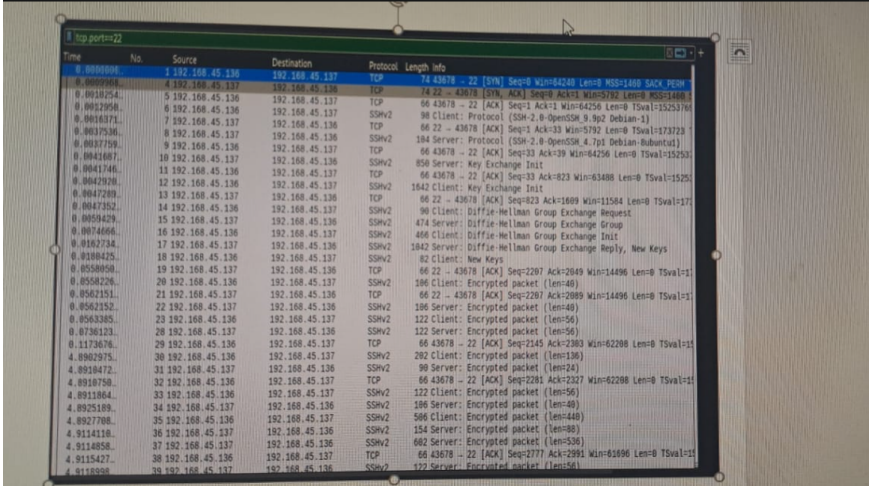
✓ Apply Filter

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



Time	No.	Source	Destination	Protocol	Length	Info
0.000000	1	192.168.45.136	192.168.45.137	TCP	74	43678 → 22 [SYN] Seq=64248 Len=0 MSS=1460 Window=0
0.001254	2	192.168.45.137	192.168.45.136	TCP	74	22 → 43678 [ACK] Seq=64256 Len=0 MSS=1460 Window=0
0.002958	3	192.168.45.136	192.168.45.137	TCP	74	43678 → 22 [ACK] Seq=64256 Len=0 MSS=1460 Window=0
0.003371	4	192.168.45.137	192.168.45.136	SSHv2	60	Client: Protocol (SSH-2.0-OpenSSH_9.9p2 Debian-1)
0.003736	5	192.168.45.136	192.168.45.137	SSHv2	60	Server: Protocol (SSH-2.0-OpenSSH_4.7p1 Debian-Rubuntal)
0.003739	6	192.168.45.136	192.168.45.137	TCP	60	43678 → 22 [ACK] Seq=33 Ack=39 Win=64256 Len=0 TSval=15250
0.004168	7	192.168.45.137	192.168.45.136	SSHv2	60	Server: Key Exchange Init
0.004168	8	192.168.45.136	192.168.45.137	TCP	60	43678 → 22 [ACK] Seq=33 Ack=823 Win=63488 Len=0 TSval=15250
0.004728	9	192.168.45.137	192.168.45.136	SSHv2	1842	Client: Key Exchange Init
0.004728	10	192.168.45.136	192.168.45.137	TCP	60	22 → 43678 [ACK] Seq=823 Ack=1609 Win=11584 Len=0 TSval=17
0.005942	11	192.168.45.137	192.168.45.136	SSHv2	90	Client: Diffie-Hellman Group Exchange Request
0.007466	12	192.168.45.136	192.168.45.137	SSHv2	474	Server: Diffie-Hellman Group Exchange Group
0.0182734	13	192.168.45.137	192.168.45.136	SSHv2	466	Client: Diffie-Hellman Group Exchange Init
0.0208425	14	192.168.45.136	192.168.45.137	SSHv2	1842	Server: Diffie-Hellman Group Exchange Reply, New Keys
0.0558958	15	192.168.45.136	192.168.45.137	SSHv2	82	Client: New Keys
0.0558958	16	192.168.45.136	192.168.45.137	TCP	60	22 → 43678 [ACK] Seq=2287 Ack=2849 Win=14496 Len=0 TSval=1
0.0562252	17	192.168.45.137	192.168.45.136	SSHv2	196	Client: Encrypted packet (len=48)
0.0562252	18	192.168.45.137	192.168.45.136	TCP	60	22 → 43678 [ACK] Seq=2287 Ack=2889 Win=14496 Len=0 TSval=1
0.0563385	19	192.168.45.136	192.168.45.137	SSHv2	196	Server: Encrypted packet (len=48)
0.0736123	20	192.168.45.137	192.168.45.136	SSHv2	122	Client: Encrypted packet (len=56)
0.1173676	21	192.168.45.136	192.168.45.137	SSHv2	122	Server: Encrypted packet (len=56)
0.8982975	22	192.168.45.136	192.168.45.137	TCP	60	43678 → 22 [ACK] Seq=2145 Ack=2383 Win=62288 Len=0 TSval=1
4.8918471	23	192.168.45.137	192.168.45.136	SSHv2	282	Client: Encrypted packet (len=136)
4.8918758	24	192.168.45.136	192.168.45.137	SSHv2	90	Server: Encrypted packet (len=124)
4.8925189	25	192.168.45.137	192.168.45.136	TCP	60	43678 → 22 [ACK] Seq=2281 Ack=2327 Win=62288 Len=0 TSval=1
4.8927788	26	192.168.45.136	192.168.45.137	SSHv2	122	Client: Encrypted packet (len=56)
4.914118	27	192.168.45.137	192.168.45.136	SSHv2	196	Server: Encrypted packet (len=48)
4.914858	28	192.168.45.137	192.168.45.136	SSHv2	586	Client: Encrypted packet (len=440)
4.915427	29	192.168.45.136	192.168.45.137	SSHv2	154	Server: Encrypted packet (len=536)
4.915538	30	192.168.45.137	192.168.45.136	TCP	60	43678 → 22 [ACK] Seq=2777 Ack=2991 Win=83896 Len=0 TSval=1
4.915538	31	192.168.45.137	192.168.45.136	SSHv2	572	Server: Encrypted packet (len=56)