



VIT[®]
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

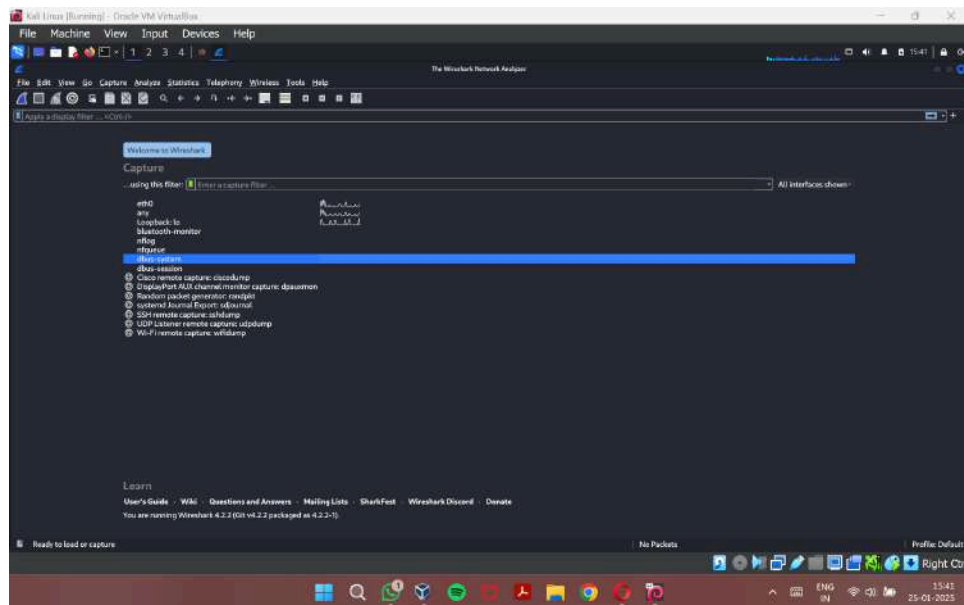
Capture ICMP and TCP traffic on **Wireshark**

NAME: DHEVATHA S P
REG NO.: 22BCE0826

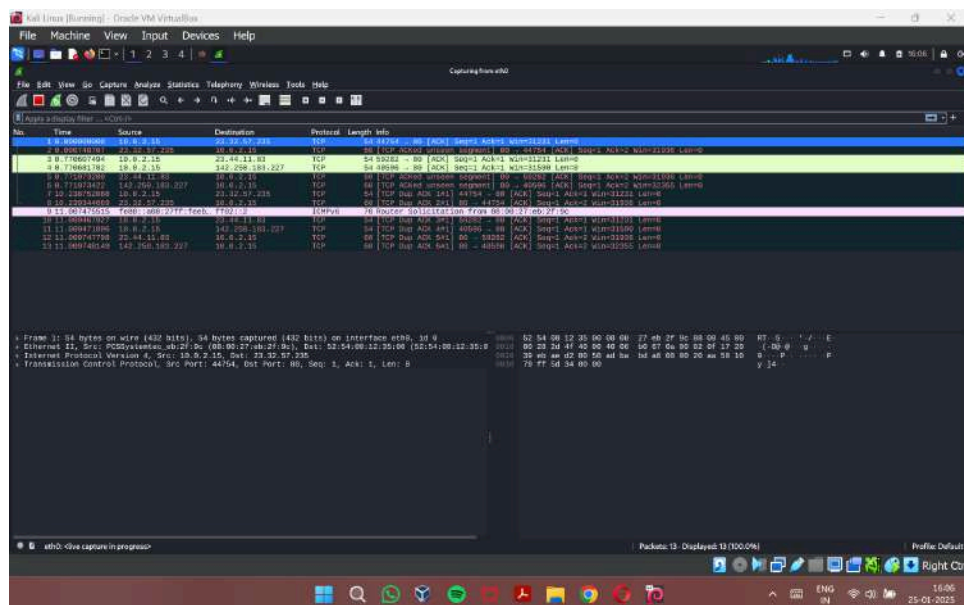
NAME OF FACULTY: DR. Satish C.J
COURSE TITLE : Penetration Testing and Vulnerability
Analysis Lab
COURSE CODE: BCSE319P
LAB SLOT: L55+L56
SEMESTER: Winter Semester 2024-25
CLASS NO.: VL2024250505928

Wireshark

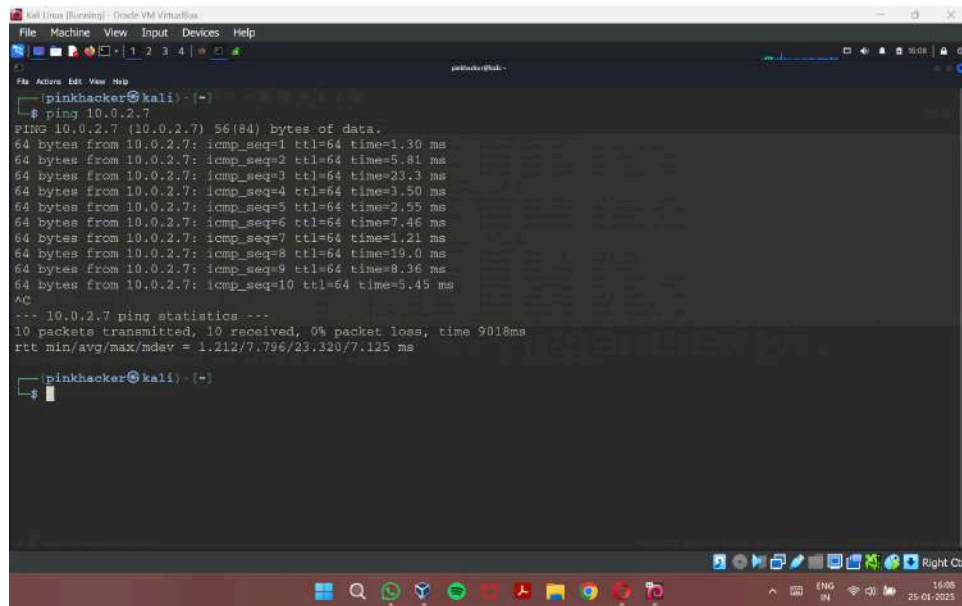
1. Open the wireshark interface in Kali Linux



2. Start capturing packets



3. Pinging the Metasploitable2 from the Kali Linux



```

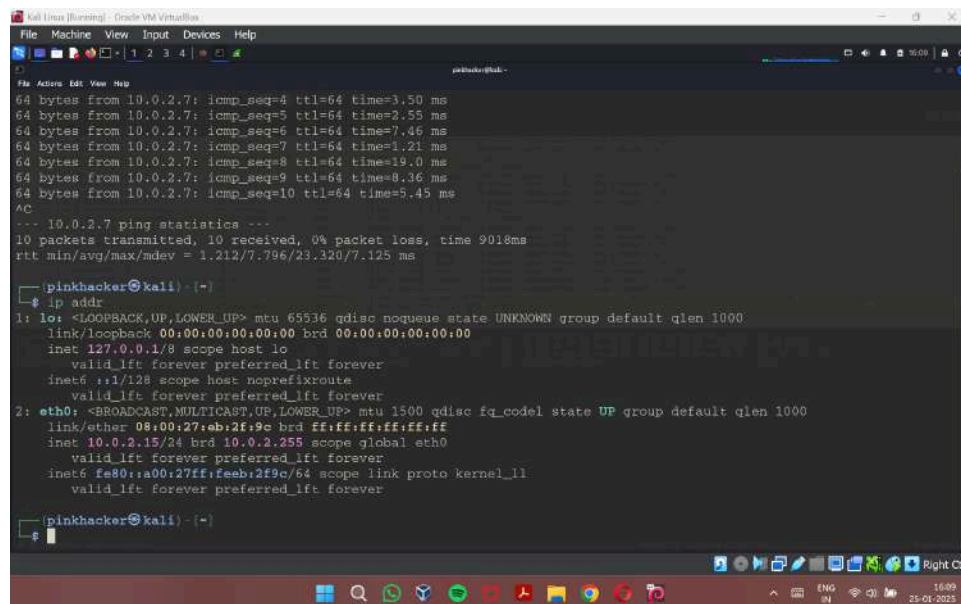
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

pinkhacker@kali: ~
$ ping 10.0.2.7
PING 10.0.2.7 (10.0.2.7) 56(84) bytes of data.
64 bytes from 10.0.2.7: icmp_seq=1 ttl=64 time=1.30 ms
64 bytes from 10.0.2.7: icmp_seq=2 ttl=64 time=5.81 ms
64 bytes from 10.0.2.7: icmp_seq=3 ttl=64 time=23.3 ms
64 bytes from 10.0.2.7: icmp_seq=4 ttl=64 time=3.50 ms
64 bytes from 10.0.2.7: icmp_seq=5 ttl=64 time=2.55 ms
64 bytes from 10.0.2.7: icmp_seq=6 ttl=64 time=7.46 ms
64 bytes from 10.0.2.7: icmp_seq=7 ttl=64 time=1.21 ms
64 bytes from 10.0.2.7: icmp_seq=8 ttl=64 time=19.0 ms
64 bytes from 10.0.2.7: icmp_seq=9 ttl=64 time=8.36 ms
64 bytes from 10.0.2.7: icmp_seq=10 ttl=64 time=5.45 ms
^C
--- 10.0.2.7 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9018ms
rtt min/avg/max/mdev = 1.212/7.796/23.320/7.125 ms

pinkhacker@kali: ~
$

```

4. IP address of the Kali Linux is 10.0.2.15



```

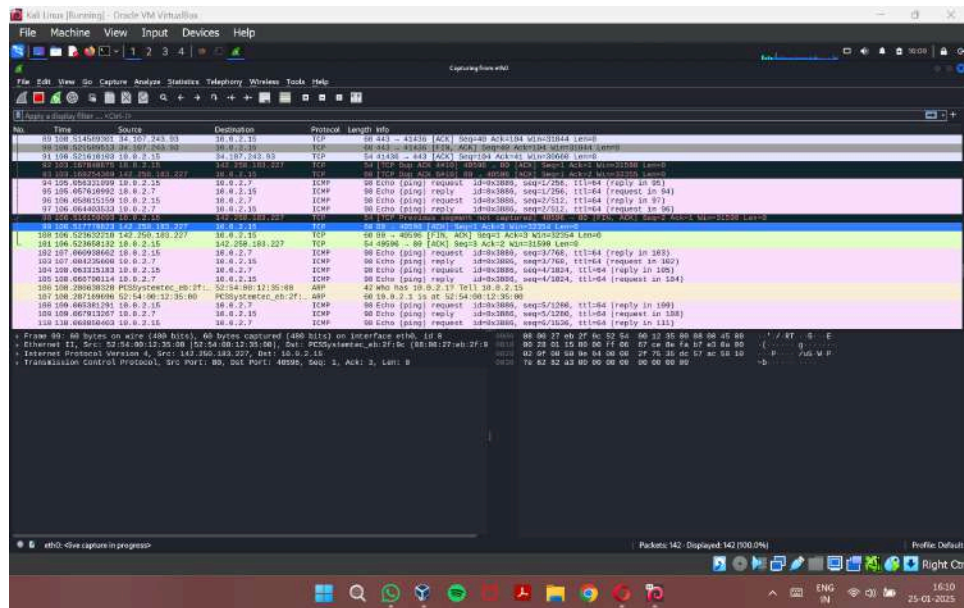
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

pinkhacker@kali: ~
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:eb:2f:9c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feab:2f9c/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever

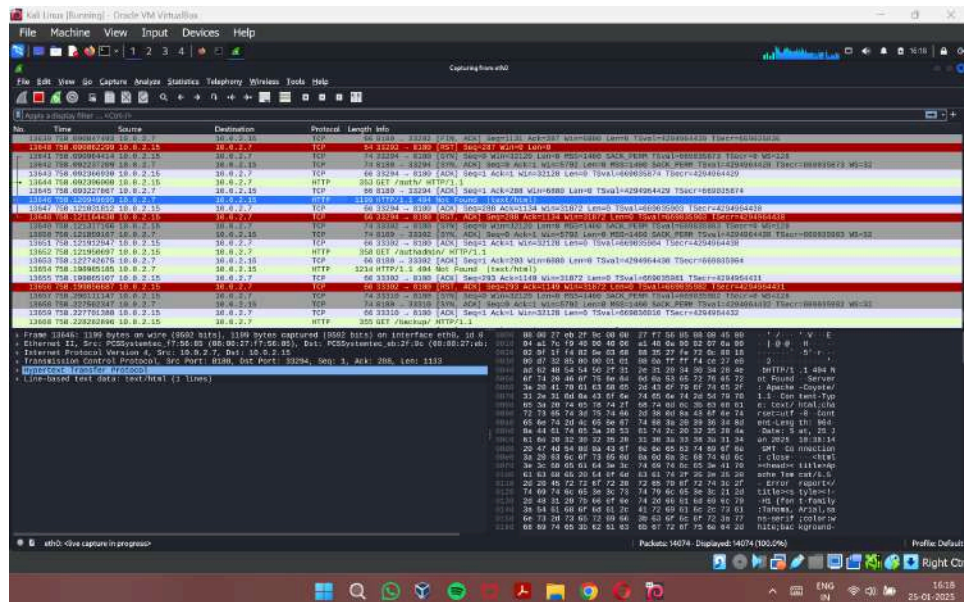
pinkhacker@kali: ~
$

```

5. The TCP 3 way handshake and the ICMP requests



6. Wireshark scan while the Nessus was scanning in parallel



Explanation:

TCP 3-Way Handshake in Wireshark

The TCP 3-way handshake establishes a reliable connection between two devices. Wireshark displays three key packets during this process:

1. SYN (Synchronization)

- Sent by the client to initiate a connection.
- Flags: SYN = 1, ACK = 0.
- Sequence Number (**Seq**): Initial random number.
- Packet Info: **TCP [SYN]**.

2. SYN-ACK (Synchronization-Acknowledgment)

- Sent by the server to acknowledge the SYN and send its own SYN.
- Flags: SYN = 1, ACK = 1.
- Packet Info: **TCP [SYN, ACK]**.
- Acknowledgment Number (**Ack**): Client's Seq + 1.

3. ACK (Acknowledgment)

- Sent by the client to acknowledge the server's SYN-ACK.
- Flags: SYN = 0, ACK = 1.
- Packet Info: **TCP [ACK]**.

By analyzing **Seq** and **Ack** numbers, you can verify successful handshakes.

ICMP in Wireshark

ICMP is used for diagnostics and error reporting. Common types include:

1. Echo Request/Reply (Ping):

- Echo Request: Sent to check host availability. (ICMP Type 8, Code 0).
- Echo Reply: Host's response. (ICMP Type 0, Code 0).
- Fields include Identifier, Sequence Number, and Data.

2. Destination Unreachable:

- Indicates network/host/port issues (Type 3).

3. Time Exceeded:

- TTL expired before reaching destination (Type 11).

Use filters like `tcp` for handshake or `icmp` for diagnostics in Wireshark. Both protocols help analyze and troubleshoot network issues effectively.