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

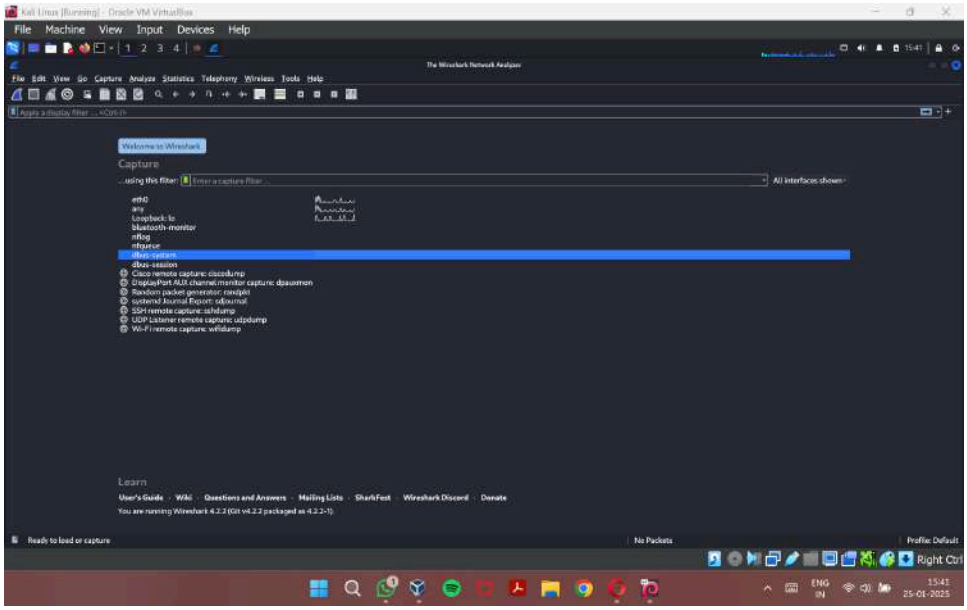
Capture ICMP and TCP traffic on Wireshark

NAME: DHEVATHA S P
REG NO.: 22BCE0826

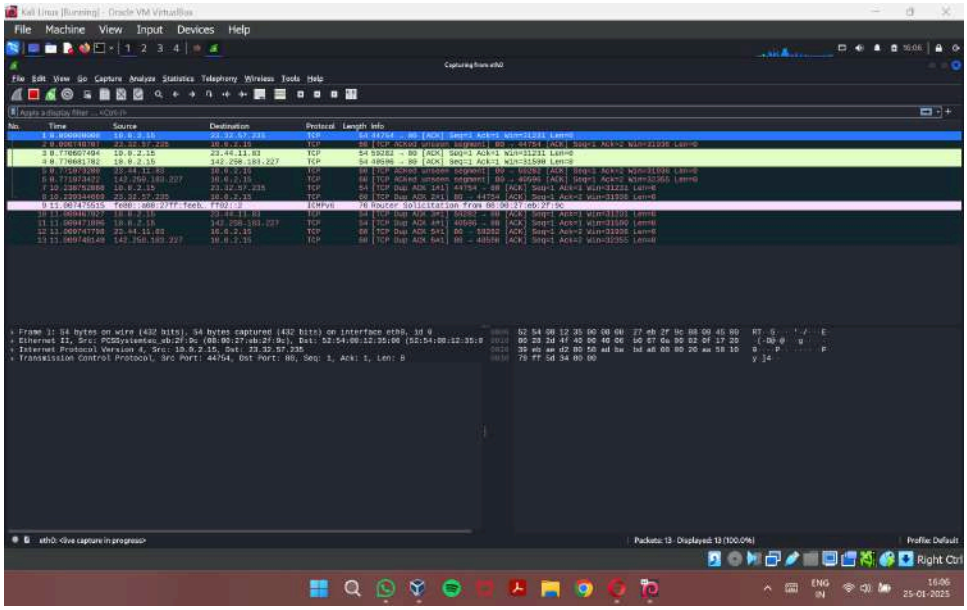
NAME OF FACULTY: DR. Satish C.J
COURSE TITLE : Penetration Testing and Vulnerability Analysis Lab
COURSE CODE: BCSE319P
LAB SLOT: L55+L56
SEMESTER: Winter Semester 2024-25
CLASS NO.: VL2024250505928

Wireshark

1. Open the wireshark interface in Kali Linux

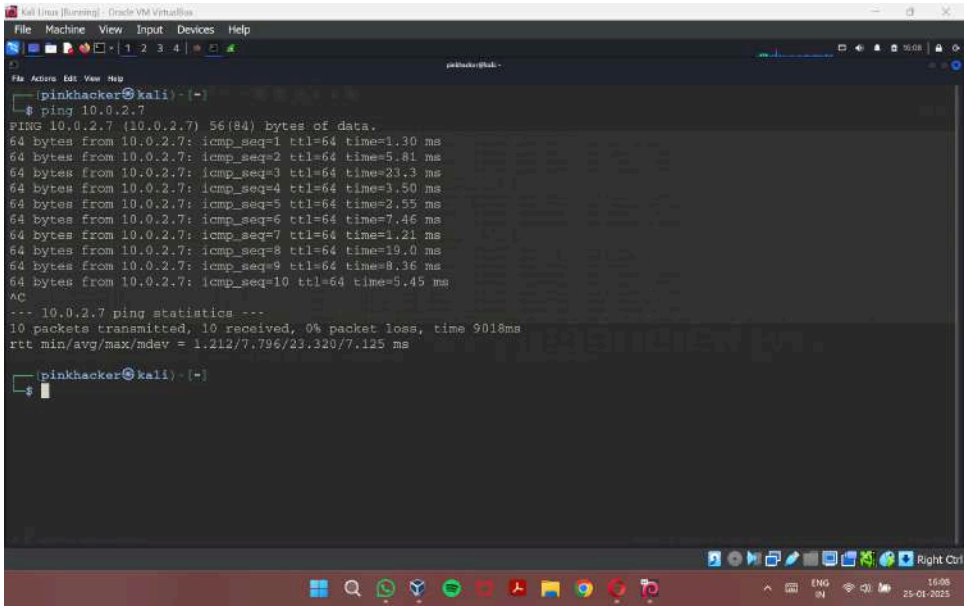


2. Start capturing packets

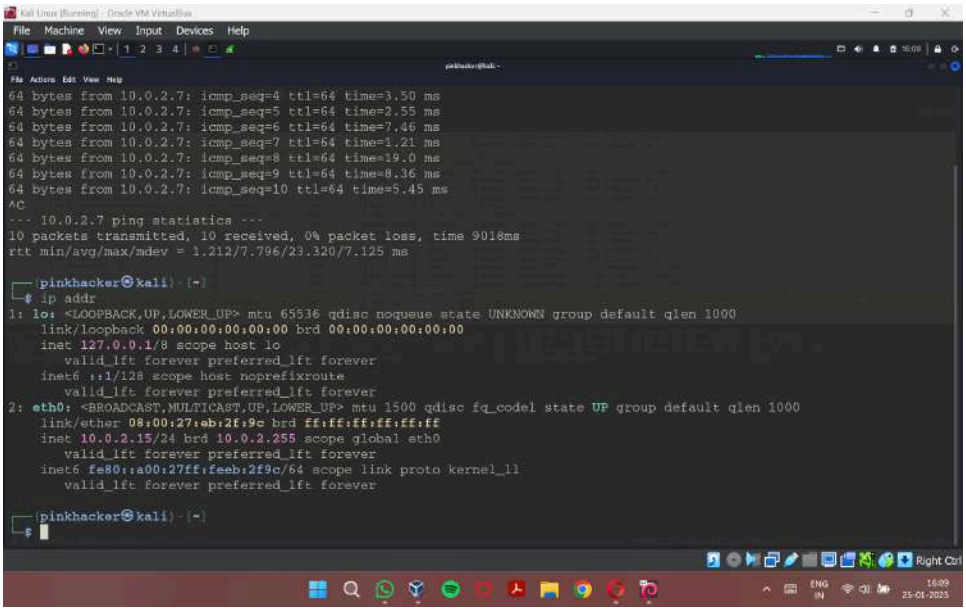


22BCE0826
Dhevatha S P

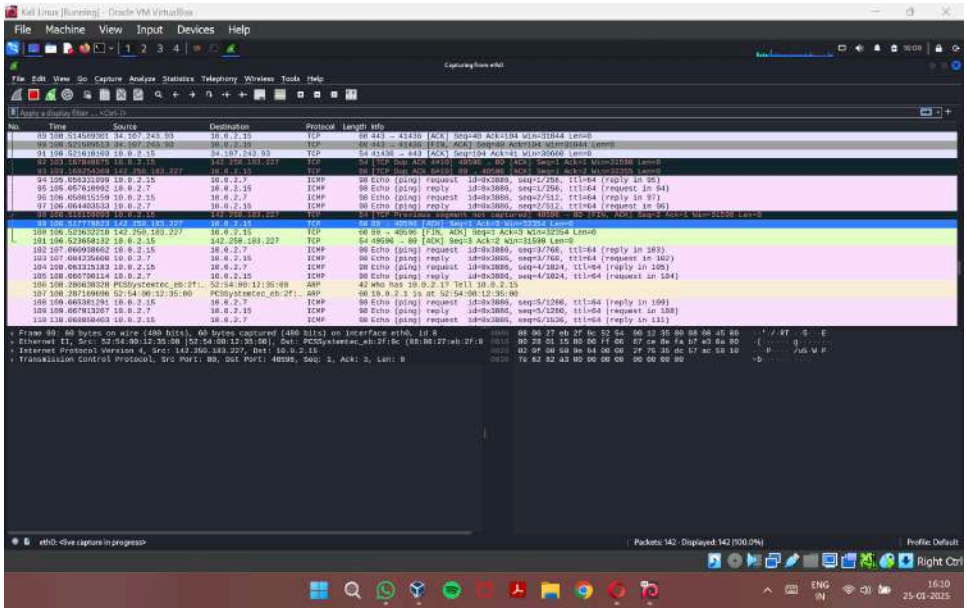
3. Pinging the Metasploitable2 from the Kali Linux



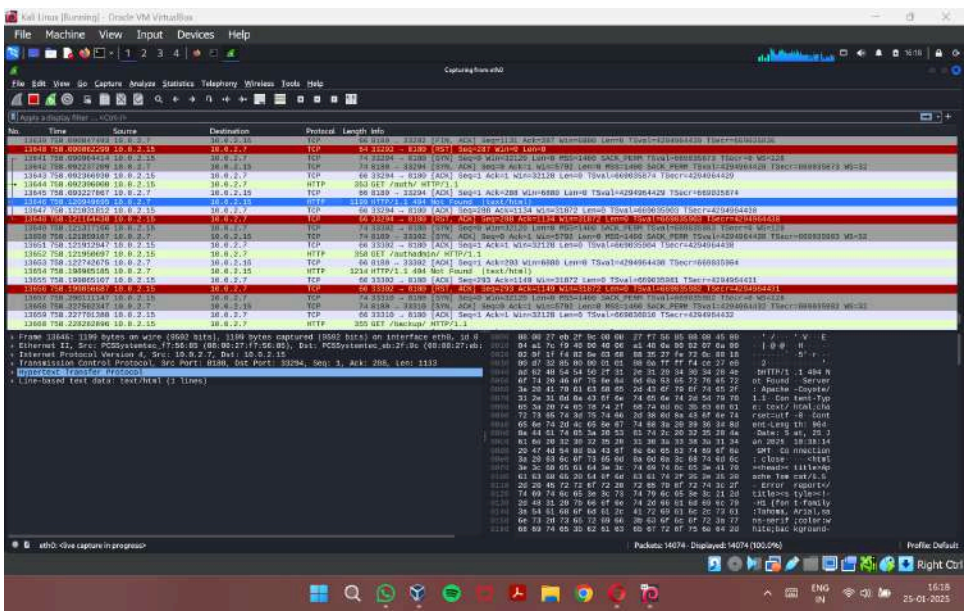
4. IP address of the Kali Linux is 10.0.2.15



5. The TCP 3 way handshake and the ICMP requests



6. Wireshark scan while the Nessus was scanning in parallel



22BCE0826
Dhevatha S P

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.