Packet Sniffing and Network Traffic Analysis

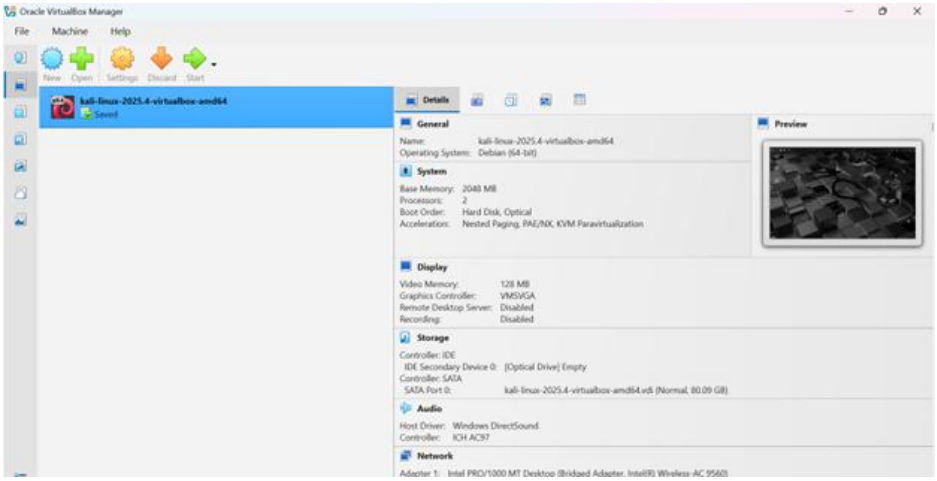
In this experiment, capture live network packets, analyze them, and understand what information an attacker can see, a local HTTP server running on port 8080 is used. Since HTTP is not encrypted, all transmitted data can be viewed in plain text by anyone who captures the traffic. Tools like tcpdump are used to capture the packets, and Wireshark is used to analyze them.

Requirements

- Kali Linux (in Oracle VirtualBox) [comes with build in Wireshark]
- Local HTTP Server (Python)

Procedure:

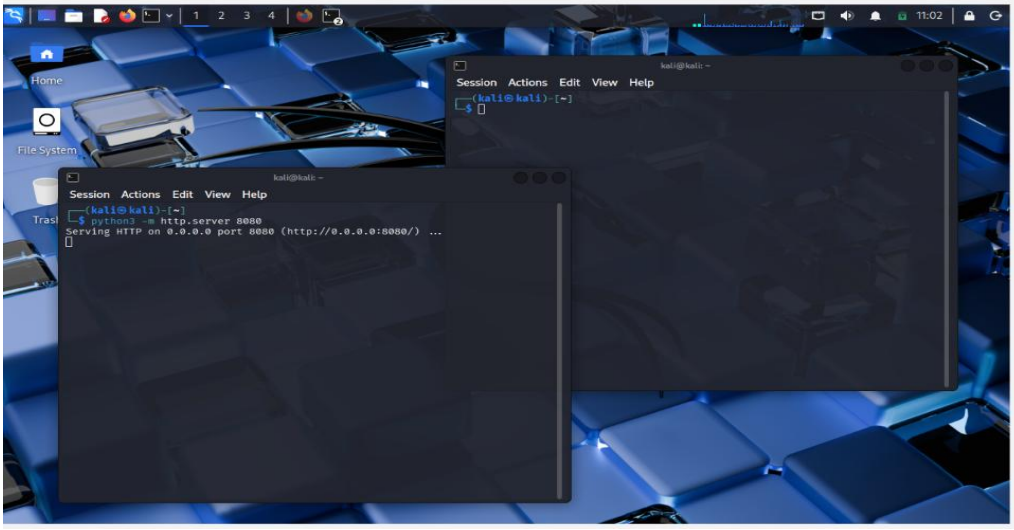
Step 1: Open Kali Linux.



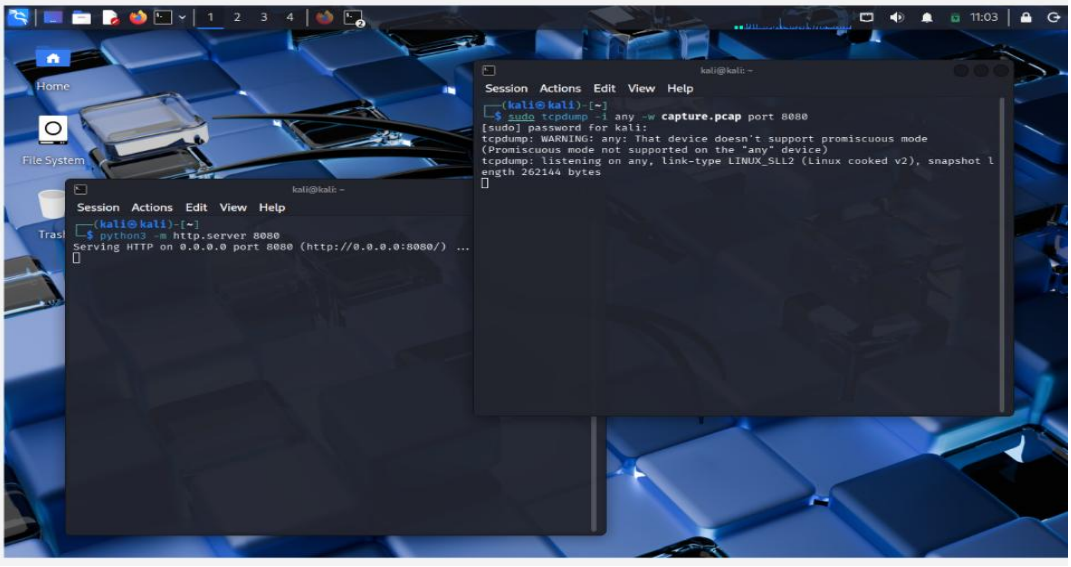
Step 2: Open Terminal in Kali Linux.

Step 3:

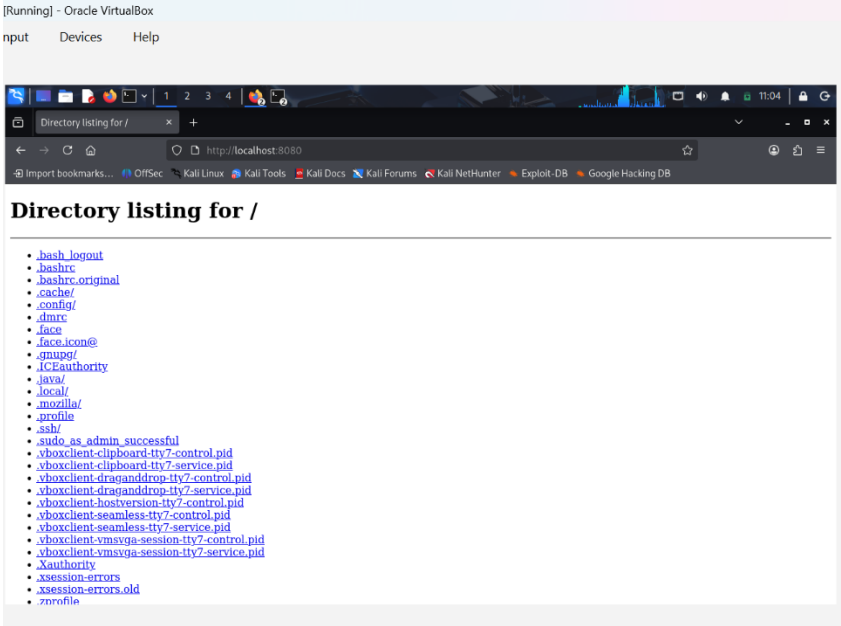
Start a local HTTP server on port 8080 using :
python3 -m http.server 8080



Step 4: In another new terminal start packet capture:
sudo tcpdump -i any -w capture.pcap port 8080



Step 5: Open Firefox in kali Linux and go to:
http://localhost:8080
Refresh the page to generate traffic.



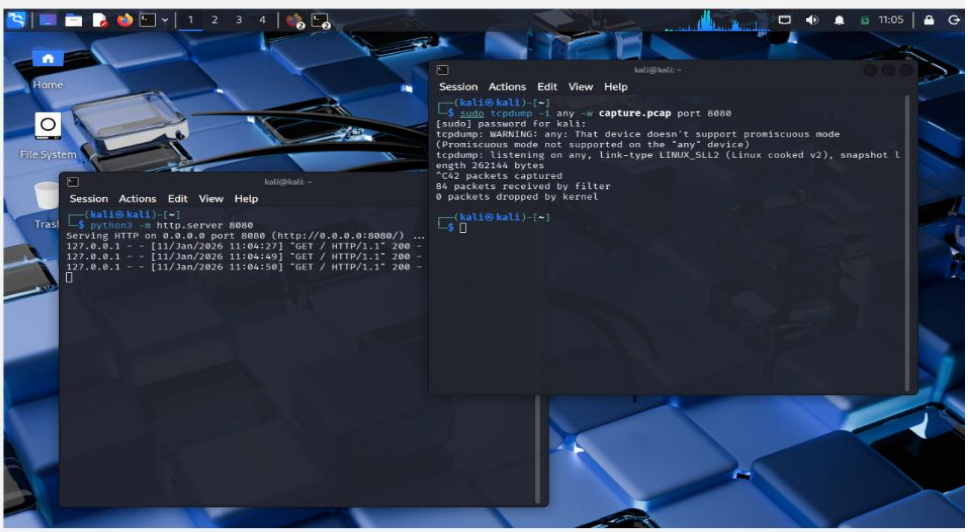
Step 6:

Go back to tcpdump terminal.

Stop packet capturing by using Ctrl + C.

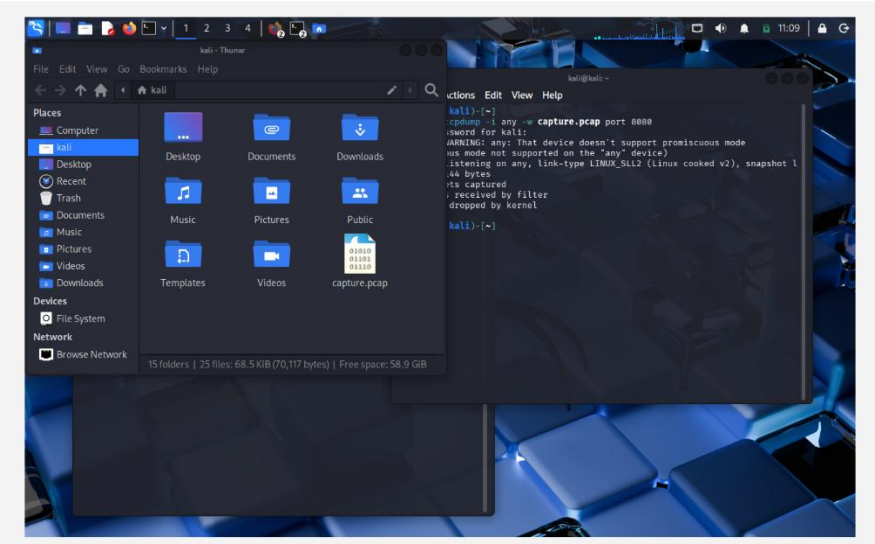
It will stop and show how many packets were captured

The packets are saved as capture.pcap.



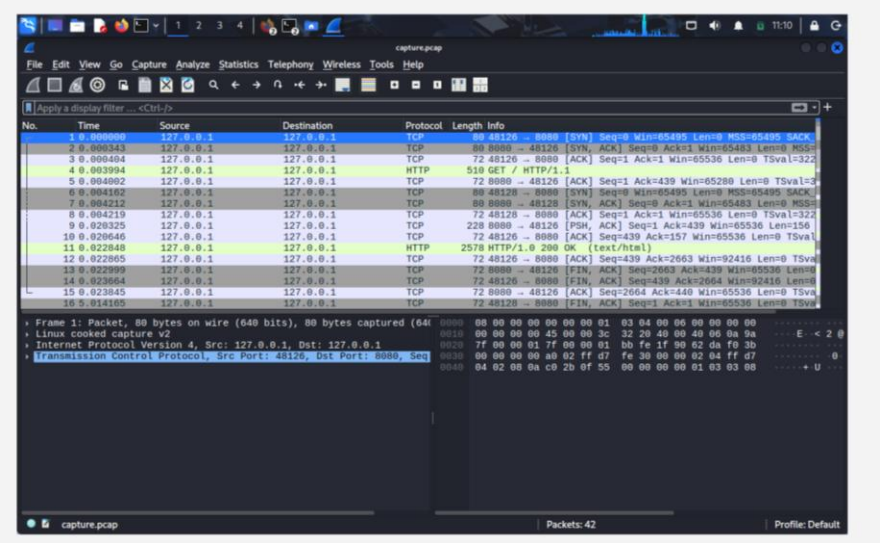
Step 7:

- Click the Kali Linux dragon icon (top left).
- Type: File Manager and open it.
- Your Home folder will open.
- You will see the file: capture.pcap.



Step 8:-

- Since Wireshark is pre-installed in Kali, just double-click capture.pcap.
- The file will open directly in Wireshark for analysis.



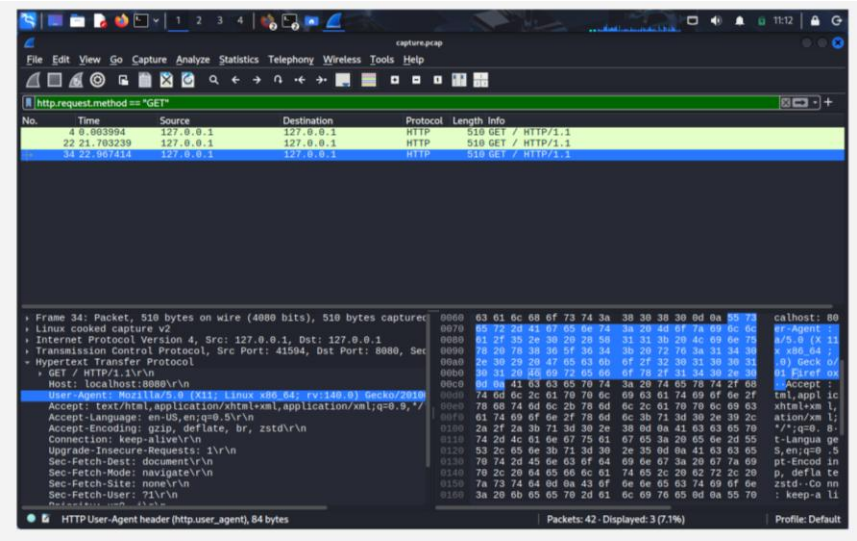
Step 9:-

Filter Login Packets

In Wireshark filter bar, type: http.request.method == "POST"

Press Enter.

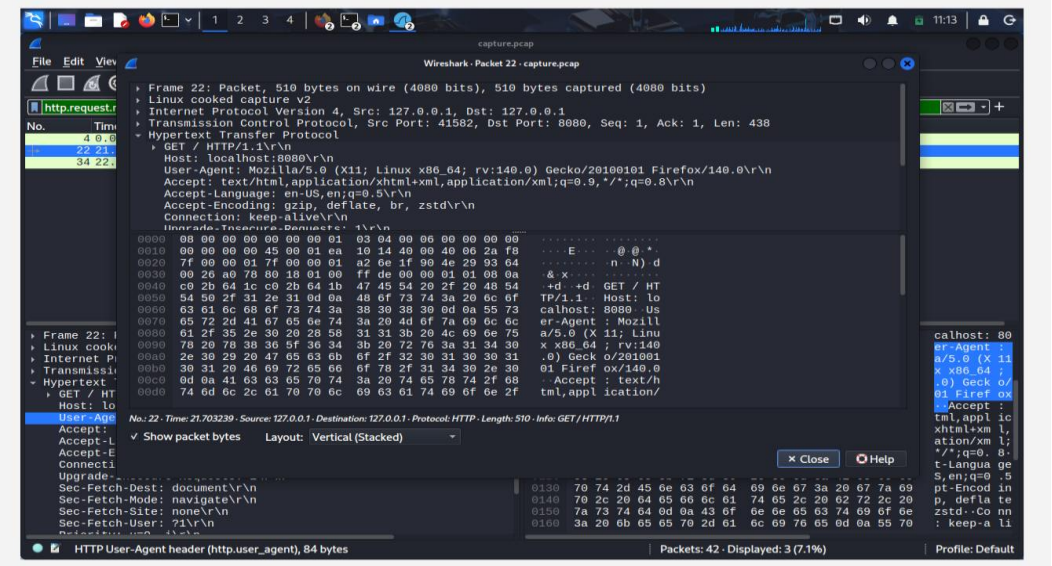
Now only important packets will show.



Step 10:-

Click on any one of the packet and the following data is displayed.

Browser details such as OS, browser version, language, and visited URLs are visible.If a form is submitted, username and password can be seen in plain text.This proves HTTP is insecure.



Conclusion :-

Packets were successfully captured and analyzed. Sensitive data is visible when HTTP is used.Packet sniffing and network traffic analysis show that unencrypted communication is unsafe. HTTPS is necessary to protect data.