Task 5 : Capture and Analyze Network Traffic Using Wireshark.

Objective: Capture live network packets and identify basic protocols and traffic types.
Tools: Wireshark (free).
Deliverables: A packet capture (.pcap) file and a short report of protocols identified

1. Install Wireshark

Wireshark is usually pre-installed on Kali, but to be sure:

sudo apt update

sudo apt install wireshark -y

🔹 2. Start Wireshark

Launch it from terminal:

wireshark

🔹 3. Start Capturing on Your Network Interface

- In Wireshark, you'll see a list of interfaces like eth0, wlan0, lo, etc.
- Look at the one with active traffic (usually wlan0 if using Wi-Fi).
- Double-click the active interface (e.g., wlan0) to begin capturing packets.

🔹 4. Generate Traffic

In a new terminal window:

ping google.com

Or open Firefox and visit: http://example.com or http://neverssl.com
(these are HTTP sites, easier to view in Wireshark).

🔹 5. Stop the Capture

After 1–2 minutes, go back to Wireshark and click the red square (stop button) on top.

🔹 6. Filter Packets by Protocol

Use the top Display Filter Bar in Wireshark:

Try these one at a time:

- http
- dns
- tcp
- icmp

You can also click the "Protocol" column to sort and identify different protocols.

🔹 7. Export the Capture File (.pcap)

- Go to File → Save As
- Name your file, e.g., kali_capture.pcap
- Save it to /home/kali/Desktop or your chosen directory.

🔹 8. Summarize Your Findings

Use this format to create a short report:

bash

CopyEdit

nano wireshark_summary.txt

Example content:

📄 Wireshark Summary on Kali

Captured Interfaces: wlan0

Total Packets: 2,300

Identified Protocols:

- DNS: 48 packets

- TCP: 1,900 packets

- HTTP: 25 packets

- ICMP: 10 packets

Interesting Points:

- DNS queries to 1.1.1.1 and 8.8.8.8

- HTTP GET request to http://neverssl.com

- ICMP replies received with ~20ms delay

Skills Practiced:

✓ Interface selection

✓ Live capture

✓ Protocol filtering

✓ PCAP export

Save and close: Ctrl + O, Enter, then Ctrl + X