■ Task 5: Capture and Analyze Network Traffic Using Wireshark ■■■■■

In this task, we used **Parrot Security OS ■** and **Wireshark ■** to capture and analyze network traffic. This exercise helps in understanding different protocols, packet structures, and network communication flow.

■ Steps Performed:

- ■ Install Wireshark on Parrot Security OS.
- ■■ Start capturing on the active network interface.
- ■ Browse a website or use the ping command to generate traffic.
- ■ Stop capture after approximately one minute.
- ■ Filter captured packets by protocol (HTTP, DNS, TCP, etc.).
- ■ Identify at least three different protocols in the capture.
- ■ Export the capture as a .pcap file.
- ■ Summarize findings and packet details.

■ Findings:
■ Identified protocols: **HTTP ■**, **DNS ■**, and **TCP ■**.
■ HTTP packets contained GET requests and responses.
■ DNS queries and responses resolved domain names.
■ TCP packets showed connection establishment and termination.

■ Conclusion:
This task demonstrated the importance of packet analysis in cybersecurity ■. By observing different protocols in action, we gain insights into network communication and potential vulnerabilities ■.