Summary Report

Title: Capture and Analyze Network Traffic Using Wireshark

Platform: Kali Linux (VirtualBox)

Objective:

To capture live network traffic using Wireshark and analyze different network protocols by filtering and exporting the packet data into `.pcap` files.

Steps Performed:

1. Installed Wireshark on Kali Linux.

2. Started packet capture on the active network interface.

3. Generated traffic using `ping` and `curl` commands to interact with different servers.

4. Stopped the capture after 1 minute and applied protocol filters.

5. Identified 5 protocols: DNS, ARP, TCP, HTTP, ICMP.

6. Saved filtered results into individual `.pcap` files.

7. Transferred `.pcap` files to Windows system using VirtualBox shared folder.

8. Prepared README and report for submission.

Protocols Identified & Packet Details:

1. DNS : 12 packets showing queries to resolve domains like `google.com` and `example.com`. Port 53/UDP used.

2. ARP : 6 packets showing MAC address resolution within local network. Example: “Who has 192.168.1.1?”

3. TCP : 30+ packets including TCP handshakes (SYN, SYN-ACK, ACK) and data exchanges.

4. HTTP : Captured GET requests and HTTP responses with status codes like `200 OK`.

5. ICMP : 10 packets including Echo Request and Echo Reply from `ping` command to `google.com`.

Tools Used:

- Wireshark

- Kali Linux Terminal (ping, curl)

- VirtualBox Shared Folder for file transfer

Conclusion:

Successfully captured and analyzed various network traffic types using Wireshark. The task provided hands-on experience in packet capturing, protocol filtering, and `.pcap` analysis. All objectives were completed, and all required artifacts have been submitted.

Submitted Files:

Task-5.zip

- dns.pcap
- arp.pcap
- tcp.pcap
- http.pcap
- icmp.pcap

README.md

Summary_Report.txt (this file)