Task Report: Capture and Analyze Network Traffic Using Wireshark

Objective

Capture and analyze live network traffic using Wireshark to identify protocols, IP addresses, and potential security issues.

Tools Used

- Wireshark - Network protocol analyzer
- Linux/Windows system with network access
- Administrative privileges to capture packets

Steps Performed

1. Install Wireshark:
   - Ubuntu/Debian: sudo apt update && sudo apt install wireshark -y
   - Windows: Download from https://www.wireshark.org/download/

2. Open Wireshark and select the active network interface (e.g., eth0, wlan0).

3. Start packet capture by clicking the 'Start Capturing Packets' button.

4. Generate network traffic by browsing websites or using applications.

5. Stop the capture after a few minutes.

6. Apply display filters to focus on specific traffic, for example:
   - http
   - tcp.port == 80
   - ip.addr == 192.168.1.5

7. Analyze packet details in the middle and bottom panes to view protocol layers and payloads.

8. Identify source and destination IPs, protocols used, and any suspicious traffic patterns.

9. Save the capture file as .pcap for future analysis.

Verification

1. Ensure packets are visible in the capture window.
2. Use 'Statistics > Protocol Hierarchy' in Wireshark to confirm protocol breakdown.
3. Cross-check suspicious IP addresses with online threat intelligence databases.

Conclusion

Wireshark successfully captured and analyzed network traffic. The analysis revealed active protocols, communicating IPs, and allowed the identification of unusual traffic patterns. This process aids in troubleshooting, performance monitoring, and security investigations.