🌐 Networking Basics for Cyber Security

📌 INTRODUCTION

This analysis report focuses on understanding **network communication** and analyzing real-time traffic using packet sniffing tools. The primary tool used is **Wireshark**, which helps capture and inspect network packets to identify protocols, traffic patterns, and security-related observations. Packet capturing and inspection were performed to observe how data is transmitted over a network and to identify secure and insecure communication.

🎯 Objectives

- Understand basic networking concepts
- Capture and analyze live network traffic
- Learn how data travels across networks
- Identify secure and insecure traffic
- Develop packet analysis skills for cyber security

📘 Networking Concepts Learned

- **IP Address:** Identifies devices on a network
- **MAC Address:** Physical address of a network interface
- **DNS:** Resolves domain names into IP addresses
- **TCP:** Reliable, connection-oriented protocol
- **UDP:** Fast, connectionless protocol

Methodology

1. Wireshark was installed on the system.

2. An active network interface (Wi-Fi) was selected.

3. Live network traffic capture was started.

4. Different protocol filters were applied to analyze packets.

5. Packet capture was saved for further analysis.

🔍 Practical Tasks Performed

✅ Step-by-Step Checklist

- Installed Wireshark successfully
- Captured live network traffic
- Applied protocol-based filters
- Observed TCP three-way handshake
- Identified plain-text vs encrypted traffic
- Captured and analyzed DNS queries
- Saved packet capture file for analysis
- Documented observations in simple language

🔎 Wireshark Filters Used

- http
- dns
- tcp
- udp

🔁 TCP Three-Way Handshake Observation

1. **SYN** – Client initiates connection
2. **SYN-ACK** – Server responds
3. **ACK** – Connection is established

🔐 Plain-Text vs Encrypted Traffic

- **HTTP:** Data is visible in plain text
- **HTTPS:** Data is encrypted and secure

🌍 DNS Traffic Analysis

- Observed DNS request packets

- Identified domain names being queried
- Analyzed DNS responses containing IP addresses

Packet Capture File

- File format: `.pcapng`

- Used for offline analysis and reporting.

Security Insights

- Unencrypted traffic can expose sensitive information.

- Packet sniffing can be used by attackers if networks are not secure.

- Encryption plays a key role in protecting data.

Conclusion

This practical task provided hands-on experience in capturing and analyzing network traffic. Wireshark helped visualize real-time communication between devices and servers. The activity improved understanding of network protocols and highlighted the importance of secure communication in cyber security.