1. Objective

The objective of this task is to understand the basic concepts of computer networking and analyze real-time network traffic using Wireshark. This task helps in understanding how data packets travel across a network and how different protocols work, which is essential in the field of cyber security.

---

2. Tools Used

- Kali Linux
- Wireshark
- Firefox Web Browser
- VirtualBox

---

3. Introduction to Networking

Networking is the process of connecting computers and devices to share data and resources. In cyber security, understanding networking is very important because most cyber attacks happen over networks.

---

4. Basic Networking Concepts

4.1 IP Address

An IP address is a unique numerical identifier assigned to each device connected to a network. It helps devices locate and communicate with each other.

Example:
`192.168.1.1`

4.2 MAC Address

A MAC (Media Access Control) address is a permanent physical address assigned to a network interface card (NIC). It is used within local networks for communication.

4.3 DNS (Domain Name System)

DNS converts human-readable domain names into IP addresses.

Example:
`www.google.com → 142.250.183.14`

4.4 TCP (Transmission Control Protocol)

TCP is a connection-oriented protocol that ensures reliable data transmission. It uses a three-way handshake to establish communication.

TCP Three-Way Handshake:

1. SYN – Client sends connection request
2. SYN-ACK – Server responds
3. ACK – Connection established

4.5 UDP (User Datagram Protocol)

UDP is a connectionless protocol that provides faster communication but without reliability. It is commonly used in video streaming and online gaming.

---

5. About Wireshark

Wireshark is a network packet analyzer used to capture and analyze network traffic in real time. It helps cyber security professionals to monitor networks, detect suspicious activities, and troubleshoot network issues.

---

6. Methodology (Steps Followed)

1. Kali Linux was started using VirtualBox.
2. Wireshark was opened and the **eth0** interface was selected.
3. Live packet capture was started.
4. Network traffic was generated by visiting websites such as Google and YouTube.
5. Packet capture was stopped after sufficient traffic was collected.
6. Different protocol filters were applied to analyze traffic.
7. The captured packets were saved as a `.pcapng` file.

---

7. Packet Analysis Using Wireshark

71 HTTP Analysis

HTTP packets were analyzed to understand unencrypted communication. HTTP data can be red in plain text, making it insecure.

7.2 HTTPS / TLS Analysis

TLS packets were observed to understand encrypted communication. HTTPS encrypts data and protects it from attackers.

7.3 DNS Analysis

DNS packets showed how domain names are resolved into IP addresses. The DNS request and response packets were clearly observed.

7.4 TCP Analysis

TCP packets were analyzed to observe reliable communication and the three-way handshake process.

---

8. Observations

- Live network packets were successfully captured using Wireshark.
- TCP, DNS, HTTP, and HTTPS protocols were identified and analyzed.
- TCP three-way handshake was clearly observed.
- DNS queries showed how websites are resolved to IP addresses.
- Encrypted HTTPS traffic was more secure than HTTP traffic.

---

9. Importance of Task 3 in Cyber Security

This task helps in understanding how attackers can sniff network traffic and how defenders analyze traffic to detect threats. It builds a strong foundation in network security and packet analysis.

---

10. Result

The task was successfully completed using Kali Linux and Wireshark. Network traffic was captured, analyzed, and documented. This task improved understanding of networking concepts and their role in cyber security.

---

11. Conclusion

Task 3 provided practical exposure to network traffic analysis. Using Wireshark, real-time packets were captured and analyzed, which helped in understanding how data flows across networks and how security protocols protect communication.

---

12. Screenshots (Attach)

- eth0 capturing packets
- HTTP filter
- DNS filter
- TCP filter
- TLS filter
- TCP three-way handshake

---

13. References

- https://www.wireshark.org
- https://www.kali.org