Task 3 – Networking Basics for Cyber Security

Detailed Practical Report (Simple English)

1. Introduction

In this task, I learned how computer networks work and how to watch network traffic using Wireshark in Kali Linux. I also learned about IP address, MAC address, DNS, TCP, UDP, and how data travels in a network. I used simple commands in the terminal and captured packets using Wireshark.

2. Basic Networking Concepts

IP Address: A unique number given to every device in a network.

MAC Address: A hardware address fixed inside the network card.

DNS: Converts website names (google.com) to IP addresses.

TCP: Reliable communication method. Uses three■way handshake.

UDP: Faster but not reliable.

3. Commands Used in Kali Linux

ip a – Shows network interfaces and their IP addresses.

ping -4 google.com – Checks internet connection using IPv4.

nslookup google.com – Finds DNS information.

dig facebook.com – Shows DNS lookup details.

sudo apt update – Updates package list.

wireshark – Opens Wireshark tool.

4. Fixing Internet Problem in Kali Linux

My Kali Linux was using IPv6, which caused internet issues. To fix the problem, I disabled IPv6 using:

```
echo "net.ipv6.conf.all.disable_ipv6 = 1" | sudo tee -a /etc/sysctl.conf

echo "net.ipv6.conf.default.disable_ipv6 = 1" | sudo tee -a /etc/sysctl.conf

sudo sysctl -p
```

After this, the ping -4 google.com command worked correctly.

5. Wireshark Practical Work

I opened Wireshark and selected the eth0 interface to capture live network traffic.

A. TCP Three■Way Handshake

Filter used: tcp.flags.syn==1

I opened example.com in the browser and saw SYN, SYN■ACK, and ACK packets.

B. DNS Query Capture

Filter used: dns

I visited google.com and saw DNS Query and DNS Response packets.

C. HTTP Traffic Capture

Filter used: http

I visited http://example.com and saw plain text GET requests.

D. HTTPS Traffic Capture

Filter used: tls

I visited https://facebook.com and saw encrypted TLS packets.

6. Saving Packet Capture File

I saved my capture as task3_capture.pcapng using:

File → Save As → task3_capture.pcapng

7. Conclusion

From this task, I learned how to capture and understand network packets. I can now identify TCP handshake, DNS queries, HTTP plain text traffic, and HTTPS encrypted traffic. This task gave me a clear understanding of how data travels across the network and how cyber security analysts use Wireshark.

(This PDF is ready for submission. Screenshots will be added in GitHub separately.)