Task 3: Networking Basics for Cyber Security – Analysis Report

Objective
The objective of this task was to understand basic networking concepts and analyze real-time network traffic using Wireshark. The task focused on identifying different protocols, observing TCP connections, and distinguishing between encrypted and unencrypted traffic.

Tools Used
Primary Tool: Wireshark
Alternative Tools: tcpdump, Microsoft Network Monitor

Methodology
Wireshark was installed and live network traffic was captured through an active network interface. Packet filtering techniques were applied to analyze specific protocols such as TCP, UDP, DNS, HTTP, and HTTPS. The captured packets were saved for further analysis.

Observations
• The TCP three-way handshake was observed using SYN, SYN-ACK, and ACK packets.
• DNS queries showed how domain names are resolved into IP addresses.
• HTTP traffic was found to be transmitted in plain text.
• HTTPS traffic was encrypted using TLS, making the data unreadable to attackers.

Security Analysis
Packet sniffing demonstrated how attackers could view unencrypted traffic. Encrypted HTTPS traffic prevents sensitive data exposure, highlighting the importance of secure communication protocols in cybersecurity.

Conclusion
This task provided hands-on experience in capturing and analyzing network traffic. It strengthened the understanding of networking fundamentals and demonstrated the role of traffic analysis in identifying security risks.

Final Outcome
The task enhanced practical skills in network traffic analysis and built a strong foundation for cybersecurity and SOC-related roles.