Task 3: Networking Basics for Cyber Security

Tool Used

Wireshark

Objective

The objective of this task was to gain a clear understanding of basic networking concepts by capturing, analyzing, and interpreting real-time network traffic using Wireshark. This task aimed to provide practical exposure to how data is transmitted across networks and how different protocols function during normal internet usage.

Observations

During this task, live network traffic was captured while browsing various websites. Multiple types of network packets were observed and analyzed to understand their roles in communication.

DNS packets were identified, which demonstrated how domain names are translated into IP addresses before establishing a connection. This helped in understanding the domain name resolution process in networking.

TCP traffic was analyzed in detail, and the three-way handshake process (SYN, SYN-ACK, ACK) was clearly observed. This process showed how reliable connections are established between a client and a server before data transmission begins.

It was also observed that HTTP traffic can be read in plain text, exposing request and response information. In contrast, HTTPS and TLS traffic appeared encrypted and unreadable, highlighting the importance of encryption in securing data. Protocol filters such as DNS, TCP, and HTTP were used in Wireshark to efficiently focus on specific types of traffic.

Security Relevance

Network traffic analysis is a critical aspect of cyber security as it helps in detecting unusual or suspicious activities on a network. By monitoring packets, security professionals can identify potential threats such as unauthorized access, malware communication, and data leakage.

Encryption plays a vital role in protecting sensitive information during transmission. Monitoring DNS traffic can also help detect access to malicious or phishing websites, making it an important technique in network security monitoring and incident detection.

Conclusion

This task improved the understanding of fundamental networking concepts and demonstrated the practical use of Wireshark in cyber security. It provided valuable insight into how network protocols operate and how traffic analysis is used to monitor, analyze, and secure network communications effectively.

Prepared By

SAFFIQMOHAMMED S