

Task 03: Networking Basics for Cyber Security

by: NROUPSINH GOHIL

Objective

The goal of this task is to understand basic networking concepts and analyze live network traffic using Wireshark. This helps in learning how data flows over a network and how attackers can observe insecure traffic.

Tools Used

- Wireshark
 - Web Browser (for generating traffic)
-

Networking Concepts Learned

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

Packet Capture Observations

1. TCP Three-Way Handshake

Observed SYN, SYN-ACK, and ACK flags which establish a TCP connection between client and server.

2. DNS Queries

DNS packets were captured showing domain name resolution when accessing websites.

3. Plain-text vs Encrypted Traffic

- HTTP traffic may expose readable information.
 - HTTPS traffic is encrypted and cannot be read directly, making it more secure.
-

Conclusion

This task provided hands-on experience in capturing and analyzing network traffic. It demonstrated how insecure protocols can expose sensitive data and why encrypted communication is critical for cyber security.