Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

Looking at the wireshark TCP/HTTP log there seems to be a SYN DoS attack this attack simulates a TCP connection and floods a server with SYN packets this attack is called SYN flooding.

Section 2: Explain how the attack is causing the website to malfunction

This attack is causing the website to malfunction because the server is being flooded with SYN packets from an out of network IP address. Since that is happening legitimate employee visitor traffic are receiving error messages indicating they cannot establish or maintain a connection to the web server. We need to block the out of network IP address that is flooding the system and configure a firewall that restricts access to out of network IP addresses to remedy this situation.