Cybersecurity Incident Report

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

SYN Flood Attack - The network traffic excerpt from the Wireshark log file reveals a pattern that strongly suggests a SYN Flood Attack. A SYN Flood Attack is a type of Denial of Service (DoS) attack in which an attacker sends a large number of SYN packets to a targeted server, overwhelming its resources and making it unable to respond to legitimate traffic.

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

The SYN flood attack is causing the website to malfunction primarily by overwhelming its resources and limiting its ability to accept legitimate incoming connections.

In a SYN flood attack, the attacker sends a large number of TCP SYN (synchronization) packets to the target system, with the intention of consuming its resources. These packets are sent with the aim of establishing a connection but are never followed through by the attacker, leaving the target system waiting indefinitely for the final handshake (ACK) to complete the connection.

As a result, the target system's resources, including memory and processing capacity, become tied up in handling these incomplete connections. This causes the server to reach its maximum connection limit, leading to the denial of legitimate connection requests from genuine users.