Cybersecurity Incident Report

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

A possible reason for the website's connection timeout error is a DoS attack. The logs reveal that the web server becomes unresponsive after being overwhelmed by SYN packet requests, indicating a SYN flooding attack.

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

When website visitors connect to the web server, a three-way handshake using the TCP protocol occurs in three steps:

1. The source sends a SYN packet to request a connection.
2. The destination responds with a SYN-ACK packet, reserving resources for the connection.
3. The source sends an ACK packet to confirm the connection.

In a SYN flood attack, a malicious actor sends a large number of SYN packets, overwhelming the server’s resources reserved for connections. This leaves no resources for legitimate TCP requests.

The logs show that the web server is overwhelmed, unable to process visitors' SYN requests, and fails to establish new connections, resulting in connection timeout messages.