Cybersecurity Incident Report

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

A potential attack that may have caused this incident of a timeout error message could be a DoS attack, specifically SYN flooding. The logs show that the number of SYN requests is greater than the server resources available to handle requests, therefore the server will become overwhelmed and unable to respond to the requests.

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

First the user tries to connect to the web server via a three-way handshake of the TCP protocol.

Three-way handshake:
Step 1: user initiates a request to connect to the web page hosted on the web server via a [SYN] packet.
Step 2: followed by step 1 the web server responds by agreeing to the connection and sends a [SYN, ACK] packet
Step 3: followed by the two steps above it finally acknowledges and allows permission to connect and makes a successful TCP connection and sends a [ACK] packet.

In a SYN flood attack the malicious actor takes advantage of the protocol by flooding the server with SYN packet requests. The number of requests is larger than the number of available ports on the server. So the server will be overwhelmed and unable to function.

By examining the logs it shows that the server is overwhelmed and unable to process user's SYN packets. Therefore is unable to get that connection and will eventually receive a timeout message.