Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
One potential explanation for the website's connection timeout error message is a DoS attack. The logs show that the web server stops responding after it is overloaded with SYN packet requests. This event could be a type of DoS attack called SYN Flood attack.

Section 2: Explain how the attack is causing the website to malfunction
When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. The handshake consists of three steps: 1. A [SYN] packet is sent from the source to the destination, requesting to connect. 2. The destination replies to the source with a [SYN, ACK] packet to accept the connection request. The destination will reserve system resources for the final step which the source will connect. 3. The [ACK] packet is sent from the source to the destination acknowledging the permission to connect. In the SYN flood attack, a malicious actor will send large amounts of SYN packets all at once, this will overwhelm the server’s available resources to reserve for the connection. As soon as this happens, There will be no server resources left for legitimate TCP connection requests. The logs indicate that the web server has become overwhelmed and is unable to process the visitors’ SYN request. The server is unable to open a new connection to new visitors who receive a connection timeout message.