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 system was flooded with SYN packets all at once. This event could be a type of DoS attack called SYN flooding.

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 three steps of the handshake include 1. A SYN packets is sent from source to destination, requesting to connect. 2. A SYN,ACK package is sent back from the destination to the source requesting to connect. The destination will reserve resources for the source to connect 3. A final ACK package is sent from the source to the destination acknowledging the permission to connect When a malicious actor sends a large number of SYN packets all at once the system is flooded with SYN packets which overwhelms the server's resources to reserve for the connection. This leaves no server resources for a legitimate TCP connection request. The logs indicate that the server has become overwhelmed and is unable to process the visitor's SYN requedts. The server is unable to establish a connection with any new visitor, who will receive a connection timeout message, even if it is a legitimate TCP connection request.