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 Denial of Service attack since the server is live but currently unable to accept connection The logs show that the web server cannot take more request after a particular visitor kept on sending SYN packets This event could be a Denial of Service perpetrated using 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 are 1. The first step is where the server receives a SYN request from the website visitor IP for a connection. 2. The second step is a SYN,ACK request sent from the server to the website visitor 3. The third step is the ACK connection sent from the website visitor to the server acknowledging the synchronized and acknowledgment connection. Thereafter further requests are made to the server for web pages or other info. In the case of a SYN flood attack, a malicious actor will send a large number of SYN packets all at once, which overwhelms the server's available resources to reserve for the connection. When this happens, there are 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 requests. The server is unable to open a new connection to new visitors who receive a connection timeout message.