Cybersecurity Incident Report

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

Section 2: Explain how the attack is causing the website to malfunction
When a website visitor try to establish a connection with the web server, it first needs to do the three-way handshake using the TCP protocol, the three-way handshake consists of the following steps: 1. A SYN packet is sent from the client side to the destination, which in this case is the web server, requesting to connect. 2. The destination replies to the client with a SYN-ACK packet to accept the connection request. The destination will reserve resources for the client to connect. 3. Finally, the client responds with an ACK packet to the destination acknowledging the permission to connect. In the case of a SYN flood attack, a malicious actor sends a large number of SYN requests to the web server, this overwhelms the server's available resources because it has to reserve resources for the client to connect. When this happens, there are no resources for legitimate TCP connection requests. The logs indicate that the web server has become overwhelmed and is unable to process the client's SYN requests, this is why the web server is unable to open new requests and a connection timeout message is received.