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 that the server is a victim of a DoS attack.
The logs show that the web server stops responding because it is being flooded with SYN packet requests.
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.

1. The first step is the client sending the server a SYN request.
2. The server then responds with a SYN, ACK request, acknowledging that it has received the request from the client to connect. The server will reserve resources for the connection. A port is also established on which the server and client communicate.
3. Finally, the client responds with an ACK message, establishing the connection between the two.

When a malicious actor sends a large number of SYN packets, the server will be trying to put resources away to establish the connection. However due to the large number of requests, the server will be depleted of its resources and unable to form a connection with a legitimate client.

The logs indicate that the server has become overwhelmed by the number of SYN packets it has received and it is unable to form a connection with a legitimate client. It is unable to process any request therefore clients are receiving a timeout error message.