Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
Potential explanation of website's connection timeout error message is DoS attack. The logs show that the server stopped responding after it was flooded by SYN packet requests. This situation can be caused by a DoS attack called SYN flooding.

Section 2: Explain how the attack is causing the website to malfunction
When the 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 resources for the source to connect. 3. A final ACK packet is sent from the source to the destination acknowledging the permission to connect. In this case the server was flooded by a large number of SYN packets on the first step of the three-way handshake. When this happened there was no place left for legitimate TCP connections. The logs indicate that the server is unable to process the visitors SYN requests due to the overwhelming amount of packets sent to it recently. The server is unable to establish a connection with a new visitor who receives a timeout message.