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 showed that the web server stopped responding after it was overloaded with SYN packet requests, implying a potential SYN flooding attack.

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. This handshake consists of three steps: 1. A SYN packet is sent from the source to the destination to request a connection. 2. The destination replies with a SYN-ACK packet in order to accept the connection request, in turn reserving resources to allow the source to connect. 3. Finally, an ACK packet is sent from the source to the destination to acknowledge the permission and establish the connection. 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 had become overwhelmed and was unable to process the visitors' SYN requests. The server was unable to open a new connection to new visitors who received a connection timeout message.