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 DoS attack is being performed, causing the web server to timeout. The logs show that the web server stops responding after being flooded with SYN requests. This event could be a TCP SYN flood attack (a type of DoS 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. Explain the three steps of the handshake: 1. SYN: The source sends a request to connect to the destination. 2. SYN-ACK: The destination responds to the SYN request that it is ready to establish a connection. 3. ACK: The source acknowledges the connection. Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a large number of SYN packets are sent, the server is overloaded as it cannot reserve enough resources to complete the connection process for each SYN request. Explain what the logs indicate and how that affects the server: The logs indicate that the web server has become overwhelmed and is unable to complete legitimate TCP connection requests.