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: The overwhelming amount of SYN requests has caused the server to become unresponsive. The logs show that: Multiple SYN requests are being sent from an unknown source IP address. This event could be: an attempt at a 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 - This is used to tell the server that the client is trying to establish a connection 2. SYN-ACK - The server then responds with an acknowledge message and a SYN of its own to reciprocate the connection. 3. ACK - Finally the client responds back with an ACK message to tell the server that the connection has been established on their end. Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a large amount of SYN packets are sent at once, the receiving server is overwhelmed and cannot keep up with the SYN requests, therefore causing it to become unresponsive. Explain what the logs indicate and how that affects the server: The logs indicate that there is an overwhelming amount of SYN requests being sent from an IP address of : 203.0.113.0, The server is then overwhelmed by the requests and cannot keep up which in turn causes it to become unresponsive.