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 SYN flood attack, which is a form of Denial-of-Service (DoS) attack. The logs show that: there was a high volume of SYN requests directed at the web server from a single IP address. This event could be: classified as a SYN flood attack, intended to exhaust the server's resources and make the website inaccessible to legitimate users.

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 client sends a SYN packet to the server to initiate a connection. 2. SYN-ACK: The server acknowledges the SYN packet by sending a SYN-ACK back to the client 3. ACK: The client responds with an ACK, and the connection is established. Explain what happens when a malicious actor sends a large number of SYN packets all at once: The server becomes overwhelmed trying to respond to each SYN packet with a SYN-ACK, allocating resources for connections that will never be completed because the attacker never sends the final ACK. Explain what the logs indicate and how that affects the server: The logs indicated repeated SYN requests without corresponding ACKs, suggesting that these were not legitimate traffic but rather a SYN flood aimed at depleting server resources.