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 TCP SYN Flood attack. This is a type of Denial-of-Service (DoS) attack where a malicious actor sends a massive number of TCP SYN packets to the web server in an attempt to overwhelm it. The logs show a high volume of SYN requests originating from a single, unfamiliar IP address, but no corresponding ACK responses to complete the TCP handshake. This indicates that the server is allocating resources to these half-open connections and is unable to process legitimate requests. This event could be classified as a SYN flood attack intended to exhaust server resources and disrupt access to the website.

Section 2: Explain how the attack is causing the website to malfunction
When users try to connect to the web server, a TCP three-way handshake is initiated: (1) the client sends a SYN packet, (2) the server responds with a SYN-ACK packet, and (3) the client finalizes the handshake with an ACK packet. In a SYN flood attack, the malicious actor sends a large number of SYN packets but never completes the handshake by sending the final ACK. This leaves the server with numerous half-open connections, tying up its resources. The logs indicate this abnormal spike in SYN requests without handshake completion, which causes the server to become unresponsive to legitimate users. As a result, employees and customers are unable to access the website, severely impacting business operations.