Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
A likely explanation for the website's connection timeout error is that the server became overwhelmed due to a Denial-of-Service (DoS) attack, specifically a SYN flooding attack. This type of attack exploits the TCP handshake process by sending a high volume of SYN requests without completing the connection, thereby exhausting server resources and preventing it from responding to legitimate users. Log analysis revealed a surge in TCP SYN requests originating from a single IP address, indicating suspicious activity consistent with such an attack. This abnormal traffic caused the server to become unresponsive, leading to the observed timeout errors.

Section 2: Explain how the attack is causing the website to malfunction
When a visitor attempts to access a website, the server and client perform a three-way handshake using the TCP protocol, which includes the following steps: (1) the client sends a SYN packet to initiate the connection, (2) the server replies with a SYN-ACK packet to acknowledge the request and allocate resources, and (3) the client responds with an ACK packet to complete the handshake and establish the connection. In a SYN flood attack, a malicious actor sends a large number of SYN packets without completing the final ACK step. This causes the server to reserve resources for incomplete connections, eventually exhausting its capacity to handle new, legitimate connection requests. As indicated in the logs, the web server is overwhelmed by these malicious SYN packets and is unable to process incoming requests, resulting in connection timeouts for legitimate users.