Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
The website's connection timeout error message may be due to a DoS attack. The server logs indicate that the web server becomes unresponsive when flooded with SYN packet requests, which could be indicative of a SYN flooding attack.

Section 2: Explain how the attack is causing the website to malfunction
When users try to connect to the web server, a three-way handshake using the TCP protocol takes place: 1. The user's device sends a SYN packet to the web server, requesting to establish a connection. 2. The web server responds with a SYN-ACK packet, acknowledging the request and reserving resources for the connection. 3. The user's device sends an ACK packet to the web server, confirming the connection. In a SYN flood attack, a malicious actor floods the web server with a large number of SYN packets simultaneously, overwhelming the server's resources for handling new connections. This causes the server to be unable to process legitimate connection requests, resulting in connection timeouts for users trying to access the website. The server logs indicate that the server is under heavy load and unable to handle the influx of SYN requests.

- Kushagra Gupta