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 that someone overwhelmed the server, leading to no response. The logs show that there was a large number of (SYN) type requests sent from one IP address This event could be DoS attack of the SYN flood type.

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 : 1. the initial request from an employee visitor trying to connect to a web page hosted on the web server. (SYN) 2.the web server’s response to the visitor’s request agreeing to the connection. The server will reserve system resources for the final step of the handshake. (SYN, ACK) 3. the visitor’s machine acknowledging the permission to connect. This is the final step required to make a successful TCP connection (ACK) When the malicious actor sends a very large number of SYN packets, initially the server tries to respond to the requests, then it sends a timeout message, and finally, it stops responding due to the cache overflow The logs indicate that it was a DoS attack carried out by a single individual.