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: The logs show that: This event could be: The company’s web server received an automated alert which indicated that while attempting to access the site, a connection timeout appeared. By using a packet sniffer to analyze the logs, we discovered a flood of TCP SYN requests were attempted from an unknown IP public address. The attack was identified as a SYN flood attack (type of DoS attack).

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.

2.

3.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:

Explain what the logs indicate and how that affects the server:

The original process of a TCP communication protocol is mainly into 3 steps known as the three way handshake. Step one is sending the SYN packet from the source network to the destination network. In second step the destination network responds by sending back the SYN packet and also an ACK packet indicating that the SYN packet is received. In the final step the source network responds by sending the ACK packet to the destination network and thus forming a secure communication channel. When a SYN flood attack is caused the destination network is flooded with numerous numbers of SYN packets. The server became overwhelmed and couldn’t respond to legitimate users. This will eventually slow down the process of the servers and effect the user experience.