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: Shows there's a large number of TCP SYN requests coming from an unfamiliar IP address. This event could be: This could be because the server has been flooded with abnormal SYN requests which cause the server to be unable to respond (SYN flood attack). This is definitely a DoS attack from a malicious actor.

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. The first step is the SYN packet request, which is sent by a source IP address that is requesting a connection with the destination or host. SYN="Synchonize" 2. The second step is [SYN, ACK] packet, is the host server responding to the request from the sender/source to establish a connection. The server will reserve system resources for the final step of the handshake. SYN, ACK stands for "synchronize acknowledge." 3.The final step is the [ACK] packet is the visitor's machine acknowledging the permission to connect. This is the final step required to make a successful TCP connection. ACK stands for "acknowledge." Explain what happens when a malicious actor sends a large number of SYN packets all at once: It becomes overwhelmed by the large volume of incoming traffic and loses its ability to respond to the abnormally large number of SYN requests which inevitably leads the web server to stop responding. Explain what the logs indicate and how that affects the server: Logs are there to show us the number of entries sent to a server and at what time they were sent. Hence you'll always

find a number and next to it the time stamp.