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:A lot of connection requests are being made to the website so the server becomes overwhelmed. The logs show that: A large number of TCP SYn requests are being made from an unfamiliar IP address. This event could be: A SYN flood 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.A TCP connection request is made from the source IP address to connect to a webpage on the host server by sending a SYN packet. 2. A SYN, ACK packet is sent from the destination IP address to the source IP address in response to the visitor’s request agreeing to form the connection. 3.An ACK packet is sent from the source IP address to the destination IP address acknowledging the permission to connect. This is the final step of TCP connection. Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor sends a large number of SYN packets the web page host server gets overwhelmed, unable to form TCP connections. Explain what the logs indicate and how that affects the server: Logs indicate a large amount of connection requests/SYN packets being sent from a certain IP address constantly. Being sent so many requests it disrupts the server functioning making it unable to form connections with requests sent from other IP addresses.