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: a lot of SYN requests were made to the server from one IP address This event could be: a Denial of Service (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. A request for connection is sent as a SYN packet from the source IP address. 2. The destination IP address replies to the request with a SYN/ACK packet accepting the request. 3. An ACK packet is then sent from the source to the destination to acknowledge the connection. Explain what happens when a malicious actor sends a large number of SYN packets all at once: It overwhelms the server with these requests and authorized sources will no longer be able to access the server’s resources. Explain what the logs indicate and how that affects the server: The server is overwhelmed and legitimate requests can no longer be processed. Timeout and error messages are now being exchanged from the server to the requesting IP address.