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 due to a DoS attack. The logs show a large number of TCP SYN requests coming from an unknown IP address which has since been blocked. This event could be caused by a SYN Flood 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. The client sends a SYN packet to the server requesting to connect. 2. After receiving the SYN packet, the server responds with a SYN-ACK packet to accept the connection request; the server then allows resources to let the client connect. 3. Lastly, the client will send back an ACK packet to the server which will acknowledge permission to connect. During a SYN Flood attack the malicious actor will send the server an abundance of SYN requests to overload the server. This will take up too many resources and prevent the server from allocating resources to legitimate TCP requests. The logs indicated a large number of TCP SYN requests from an unfamiliar IP address. This overwhelmed the server due to the volume of incoming traffic and lost its ability to respond to the clients.