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 server is unable to establish a connection due to the large number of Synchronize(SYN) Packets being sent to the server. The logs show that: An abnormal number of SYN packets are being sent to the server via port 443(Encrypted web traffic) This event could be: A SYN flood DoS attack on the server.

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. 2. The server acknowledges receipt of the SYN packet by sending back a SYN/ACK(Synchronize acknowledge) packet back 3. The Client then sends back an ACK packet and a TCP conection is established. Explain what happens when a malicious actor sends a large number of SYN packets all at once: The server gets overwhelmed trying to respond to SYN packets all at once causing the server to overload. Explain what the logs indicate and how that affects the server: The logs indicate an abnormally large number of SYN packets being sent every few milliseconds causing the server to be overwhelmed in trying to respond to every request.