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: this is a SYN flood DoS attack, and the server is timing out and not responding. This event could be: a DoS attack by 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. Src sends a SYN packet to the server 2. Server responds with a SYN/ACK packet 3. Src responds with ACK packet and then a TCP connections is established between the host and server. Explain what happens when a malicious actor sends a large number of SYN packets all at once: the server tries to handle them by sending multiple SYN/ACK packets but as the number increases heavily the server begins to slow down and eventually stop responding. Explain what the logs indicate and how that affects the server: the servers indicate multiple SYN/ACK packets in the span of 3 - 4 seconds and after that the server stopped responding looking at the logs it can be deduced that the server stopped responding until the 29 sec.