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 web server was overwhelming with flooding SYN packets The logs show that: a large number of TCP SYN requests coming from an unfamiliar IP address. This event could be: 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. Device sends SYN request to server 2. Server then responds with a SYN/ACK packet to acknowledge the receipt of the device's request and leaves a port open for the final step of the handshake. 3. Server then receives the final ACK packet from the device, a TCP connection is established after that. Explain what happens when a malicious actor sends a large number of SYN packets all at once: When there are a larger number of packets sent to the server, and the server doesn't have enough ports to receive, then the server will be overwhelmed and unable to function normally.