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 large number of TCP SYN requests are coming from an unfamiliar IP address. This event could be: A 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.The initiating device sends a packet to the device it would like to connect to. 2. The device we are trying to connect to acknowledges the request and willingness to connect. 3.The initiating device sends a TCP packet with the acknowledgement and the connection is established. Explain what happens when a malicious actor sends a large number of SYN packets all at once: The malicious actor has flooded the network causing the connecting device to be overwhelmed. When a malicious actor sends a large number of SYN packets all at once, this overwhelms a system by there being a high number of SYN requests that have not completed the three-way handshake. Explain what the logs indicate and how that affects the server: The logs indicate that a DoS SYN flood attack has occurred which has made the web server stop responding to legitimate visitor traffic.