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 down due to a malicious attack or misconfiguration and can't respond to the requests. **The logs show that:** The server receives multiple SYN requests from the same source in a short period of time. After some time, he failed to handle with all of them. **This event could be:** A DOS attack, a malicious actor is trying to shut down the website.

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. SYN – Client requests server to open a connection. 2. SYN + ACK – Server respond to client with ACK to indicates the possibility of establishing the connection. 3. ACK – Client and server both establish a reliable connection. **Explain what happens when a malicious actor sends a large number of SYN packets all at once:** With a large number of SYN packages all at once the server resources will be overload and loose de capacity to respond to any inbound request. **Explain what the logs indicate and how that affects the server:**
The log indicates multiple inbound SYN requests from the same source IP, provoking a overload of server capacity to respond to users requests.