# 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:<br><br>The logs show that: There is an abnormal amount of SYN request to the network.<br><br>This event could be: it could be a SYN flood attack since there is an abnormal amount of SYN request. |

| **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:<br>1. The source device would first send a SYN request to the destination.<br><br>2. The destination would then respond with SYN-ACK to acknowledge the receiving device.<br><br>3. The source then receive that SYN-ACK and then send a ACK packet to confirm with the destination device.<br><br>Explain what happens when a malicious actor sends a large number of SYN packets all at once: if a large number of SYN packets are sent all it once, the web server will struggle to keep up with it which then starts sending error messages.<br><br>Explain what the logs indicate and how that affects the server: The logs indicates that there is a SYN flood attack which cause the server to start sending error messages. |