# 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: We are under a SYN flood attack<br><br>This event could be: Detrimental to business continuity |
| |

| **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. A SYN Packet is sent by the client.<br><br>2. The server responds with a SYN-ACK packet<br><br>3. The client acknowledges with an ACK packet.<br><br>Explain what happens when a malicious actor sends a large number of SYN packets all at once: **they are essentially overwhelming a target server with connection requests, causing it to become overloaded and unable to respond to legitimate traffic**<br><br>Explain what the logs indicate and how that affects the server: There were many repeated SYN requests sent until service was denied. Access to the web site will be denied until the issue discontinues or is resolved. |
| |