# 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 TCP is not responding because it is overwhelmed  The logs show that: There are numerous SYN requests in quick succession in the TCP protocol coming from the same IP Address  This event could be: This could be reflective of a IP spoofing attack and a Dos Attack in the form of SYN 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. Originating PC send SYN packet to TCP server.  2.TCP Server sends SYN/ACK to the originating IP Address;  3.Originating IP address sends an ACK packet back to the TCP server confirming the handshake  Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor sends large number of SYN packets in short succession, the TCP server becomes overhwelmed and is unable to respond before being overloaded.  Explain what the logs indicate and how that affects the server: The logs are indicating that there is 1 IP Address that is sending SYN packets to the TCP server and is being done in short succession (several within seconds) |