# 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: TCP SYN attack  The logs show that: An abnormal amount of syn request are being sent  This event could be: A DOS 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.syn request is sent from client  2. server receives syn request and sends syn/ack to client  3.client receives syn/ack and sends ack  Explain what happens when a malicious actor sends a large number of SYN packets all at once: it overloads the system and keeps it from performing normal task.  Explain what the logs indicate and how that affects the server: That legit traffic is not connecting because of attackers flood of syn request. |