# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| The explanation for the website’s connection timeout is because the server is attacked by a malicious actor, the logs show a ridiculous amount of TCP SYN requests from an unfamiliar IP Address, this might be a DoS attack specifically a SYN flood attack. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| The three steps of a handshake is   1. The user/visitor sends a initial request to the web server by sending a SYN packet when trying to connect to a webpage. 2. The web server responds by agreeing to the user’s request, reserving system resources and sending back a SYN ACK packet. 3. The ACK packet is acknowledged on the user’s machine granting permission to connect, this is the final step to establish a TCP connection.   The web server would be overwhelmed by the amount of SYN packets it’s receiving which results to a slowdown and eventual crash, we know that the system reserves system resources when trying to perform a handshake even if a unfamiliar IP address requests it.  The logs indicate a SYN flood attack by sending an abnormal amount of SYN packets to the web server which affects the performance of the server in handling requests which ultimately proceeds to a crash, or a shutdown performed manually by a cybersecurity professional to mitigate the attack. |