# 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 web server is taking a long time to respond to the client's requests for the webpage possibly a Dos attack has been made.  The logs show that: A lot of TCP Syn requests are being sent from an unfamiliar IP address continuously which has caused an overload and the web server has stopped responding.  This event could be: A Dos attack namely a SYN flood 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 meaning synchronize which is first sent from the client to the web server requesting a connection.  2. SYN- ACK meaning synchronize - acknowledge which is sent by the web server to the client agreeing to the connection.  3. ACK meaning acknowledge which is sent from the client to the web server which acknowledges the permission provided to connect.  **Explain what happens when a malicious actor sends a large number of SYN packets all at once:**  The Web server with too many SYN requests overwhelms the server’s available resources to reserve for the connection. When this happens, there are no server resources  left for legitimate TCP connection requests.  **Explain what the logs indicate and how that affects the server:**  The logs indicate lots of SYN connections being requested from the web server because of which the web server has stopped responding, which affects the server's network bandwidth. |
|  |