# 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 logs show that: there is a large amount of SYN packet request from a single user that causes the web server to stop responding to authorized requests  This event could be a DOS attack called SYN flooding | |
|

| **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. The three steps of the handshake:  1. A SYN (synchronization) packet is sent from source to destination , requesting to establish a connection  2. The destination will reply the source with a SYN/ACK packet (synchronized/ acknowledge) to indicate that it has accepted the request , and it will reserve resources while waiting for the source to connect  3. The source will then send a final ACK packet to the destination acknowledging permission to connect  When a malicious actor sends a large number of SYN packets all at once , the server will be overwhelmed and the available resources will eventually run out just to reserve the resources for the connection. When this happens , the server cant respond to authorized / legitimate requests because there are no server resources left.  Explain what the logs indicate and how that affects the server: The logs indicate that the server is flooded with SYN packets from a malicious actor , and the server cant process new SYN request from visitors thus causing the visitor to receive timeout errors such as HTTP/1.1 504 Gateway Time-out (text/html) and [RST, ACK] packet. |