# 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 a DOS attack.The logs show that, large number of TCP SYN requests are coming for unfamiliar IP address. Because of this, the web server is overwhelmed by the volume of incoming traffic and losing its ability to respond. This event could be a type of 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.   1. A SYN packet is sent from source IP address to Destination IP address, requesting for a TCP connection. 2. If the SYN packet from source IP address is confirmed by Destination IP address, Destination IP address then replies with a SYN-ACK packet to accept the TCP connection. The destination IP address reserves its resources for the source to connect. 3. A final ACK packet from source IP address to the Destination IP address acknowledging the permission to connect.   When a malicious actor sends a large number of SYN packets all at once, it overwhelms the web server’s available resources to reserve a connection. If there are no resources left reserved for the next legitimate TCP connection request, It can crash the web server causing the organization a downtime in the operations instead of making profits.  The logs indicate that the web server has become overwhelmed with the large number of TCP SYN requests coming and unable to host other legitimate TCP SYN requests, instead new visitors receive a connection timeout message. |