# 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 malicious actor performing a DOS SYN flood attack on the server. The logs show that multiple SYN requests are coming from a particular IP address without acknowledging. This event could be a DOS 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. First the requester will send a SYN packet to the server to request a connection   2. Then the server sends a SYN/ACK packet to confirm it received the sender's connection request and acknowledges the same.  3. At last the requester will send an ACK packet to the server to complete the 3-way handshake process and the connection is formed  Explain what happens when a malicious actor sends a large number of SYN packets all at once: The server will try to assign all the ports available to accommodate all the requests sent by the attacker and will be waiting for the attackers response to no avail. This will make the server unable to respond to requests of legitimate users.  Explain what the logs indicate and how that affects the server: The logs will help us to see which Ip address is the problem as we can analyze and it’s even color coded for our ease of use. |