# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this network interruption** |
| --- |
| A possible explanation for the website's connection timeout is a SYN flood attack (DOS). The logs show that the source IP address 203.0.113.0 sent an unusually high amount of SYN requests to the web server. This event could be caused by a malicious actor exploiting the TCP protocol. |

| **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. First the source IP sends a SYN request to the web server, next the server responds with an SYN ACK which acknowledges the SYN request sent by the source IP. Finally the original source IP sends an ACK packet back and the connection is established.<br><br>A malicious attacker can take advantage of this process and send multiple SYN requests at once which will result in the network becoming flooded with unwanted traffic. If enough requests are sent the network will become overwhelmed and users will not be able to connect.<br><br>In this instance, the logs indicate that IP address  203.0.113.0 sent over 140 SYN request to the web server at 192.0.2.1 within 51 seconds. This is overwhelming the web server causing it to be unreachable by legitimate users SYN requests. |