# 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 due to the abnormal SYN requests. The logs show that there are too many SYN requests being sent from a particular IP (203.0.113.0). The volume is overwhelming the resources of the web server leading to other potential connections not getting ACK response for their hand shake requests thus no connection can be established. This event could be termed a SYN flood/DOS 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:  The client system sends a SYN request to the web server. upon receipt of this request the server acknowledges and sends a SYN ACK response, the client responds to this by sending another ACK and the connection is established.  When a large number of continuous SYN requests are sent to the server, if the requests overwhelm the server resources. The server will not be able to acknowledge requests from other clients thus a TCP connection cannot be established. When this happens the webserver resources cannot be accessed leading to Gateway timeout or RST error.  Log indicates (203.0.113.0) IP is sending a Syn flood to bring down the server by exhausting its system resources. This has led to gateway timeout and RST error messages. |