# 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 type SYN flood attack is occuring from ip 203.0.113.0, the server never receive the final step of handshake which is ACK packet  The logs show that ip source 203.0.113.0 are constantly sending a SYN request to 192.0.2.1 without further data (no page requested)  This event could be DoS attack type 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. device requesting a handshake TCP[SYN] to server informing that device is requesting a establish a connection  2. server respond to client request with TCP[SYN, ACK] Acknowledge, identifying that the server acknowledge the synchronize request and start a segment with client  3. In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer  Explain what happens when a malicious actor sends a large number of SYN packets all at once: A SYN flood attack affects a server by consuming its connection resources and making it unresponsive to legitimate users. The server is bombarded with connection requests (SYN packets) that are never completed, leaving the server with many half-open connections that deplete memory and CPU  Explain what the logs indicate and how that affects the server: logs that indicate the attack were the threat actor (203.0.113.0) send a request for a handshake with the server [SYN] and the server respond to the request [SYN, ACK]. However there were no further action, the server is not receiving any final step of the handshake which is [ACK] from 203.0.113.0, this consumed the server resources with a half opened connection. |