# 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: multiple requests to establish a TCP connection, otherwise known as a SYN flood attack  The logs show that: There are many TCP SYN requests coming from the IP 203.0.113.0, which is overwhelming the web server’s ability to process legitimate requests.  This event could be: The results of a Denial-of-Service attack, all the SYN requests come from 1 device which eliminates the option of it being a Distributed DoS attack. The large number of SYN requests are larger than the number of ports available which has in turn disbaled the server from taking any more requests and anyone that does access the website will be met with gateway timeout message |
|

|  |
| --- |
| **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. A SYN packet is sent as the initial request to the web server   2. The web server will respond with a [SYN, ACK] packet as an agreement to the connection. The server will begin to reserve system resources for the final step  3. The ACK packet is sent back to the web server as an acknowledgement of their permission to connect. This establishes the TCP connection.  Explain what happens when a malicious actor sends many SYN packets all at once:  The server allocates resources for each SYN request, sending out a SYN/ACK packet. The server will wait for the ACK packet to complete the handshake but when it never arrives the server is left with open connections that consume the servers’ resources and port spaces which will overwhelm the server and prevent it from making any further connections  Explain what the logs indicate and how that affects the server:  The logs show that there are many SYN requests coming from 1 IP address that progressively overload the server, leaving many open connections. Eventually there are no free ports for any legitimate connections. |