# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| A network outage occurring on a website is a surge in TCP SYN requests coming from a single IP address. Therefore, this is a network level denial of service (DoS) attack, called a SYN flood attack, that targets network bandwidth to slow traffic. This form of attack floods a web server with incomplete connection requests, overwhelming its resources and hindering its ability to effectively handle legitimate user connections. |
|

|  |
| --- |
| **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:  The first step in the handshake is for the device to send a SYN, or synchronize, request to the server. Then, the server responds with a SYN/ACK packet to acknowledge the receipt of the device's request and leaves a port open for the final step of the handshake.  A malicious actor will send a large number of SYN packets all at once, which overwhelms the server’s available resources to reserve for the connection. When this happens, there are no server resources left for legitimate TCP connection requests.  This prompted us to temporarily take the server offline and implement IP blocking as an initial countermeasure. |