# 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:  The logs show that: Over the course of 7ms there was one complete SYN/ACK handshake between our local server at ‘192.0.2.1’ and a potential threat at ‘203.0.113.0’. After the handshake the threat sent a series of several SYN requests per second before awaiting acknowledgement.  This event could be: SYN flood attack from malicious threat actor. | |
|

| **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. Synchronization (SYN) request from source endpoint as a show a connection wishes to be established 2. Synchronization Acknowledgement (SYN/ACK) response from destination endpoint 3. Acknowledgement (ACK) response from the source endpoint to begin connection   Explain what happens when a malicious actor sends a large number of SYN packets all at once: The requests overwhelm the destination endpoint making services unavailable.  Explain what the logs indicate and how that affects the server: The logs show that there was a volley of SYN requests from the same address that caused the server’s requests to time out. |