# 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: One IP address is pushing multiple Synchronization requests, which flood the system and is causing the system to lock up.  This event could be: a SYN Denial of Service attack against the Server. |
|

|  |
| --- |
| **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. Step 1 is the SYN or Synchronize step  2. Step 2 is the Synchronize Acknowledge (SYN ACK) step in which the server acknowledges the receipt of the issue and reserve the system resources for the final step.  3. Step 3 is the Acknowledging (ACK) in which the system provides permission to connect. This is the final step to engage a TCP connection.  Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a large number of SYN Packets are sent at once, the Server is overloaded with requests which locks out any other users and prevents the resource from being accessed.  Explain what the logs indicate and how that affects the server: The logs begin with regular traffic, but as the SYN Requests from the IP Address 203.0.113.0 increases over time it’s causing the server to be stuck in a Synchronization Loop in what looks to be a SYN Attack Denial of Service from a single IP Address. The Server is now in a state of panic and the server is not responding to anyone at this time. |