# 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 SYNflod attack, which is a type of Denial o Service (DoS) attack where the attacker sends a large number of SYN requests to a server without completing the three-way handshake.  The logs show that the IP address 203.0.113.0 repeatedly sends SYN packets to port 443 of the server at 192.0.2.1 without completing the handshake, as indicated by the lack of ACK responses.  This event could be a 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.   1. SYN: the client sends a SYN packet to the server to initiate the connection 2. SYN-ACK: the server responds with a SYN-ACK packet 3. ACK: the client sends an ACK packet to the server, acknowledging the receipt of the server’s SYN-ACK packet.   When a malicious actor sends a large number of SYN packets all at once without completing the three-way handshake, it creates an attack known as SYN flood. For each SYN packet, the target server allocates resources to handle what it believes is a legitimate connection. This includes reserving memory and maintaining half-open connections while waiting for the ACK packet to complete the handshake. As more SYN packets flood the server, the number of half-open connections increases, consuming more server resources. Eventually, the server becomes overwhelmed, running out of memory or connection slots to handle legitimate traffic.  The logs show a first SYN packet a 3.144521 seconds after starting capturing the network logs. By that time, the server was still responding other requests. However, from 21.136783 seconds, the server stopped responding, and only incoming SYN packets is found in the log. |