# 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 SYN flood attack, where an attacker sends a high volume of TCP SYN requests to overwhelm the web server, leading to resource exhaustion and a subsequent connection timeout error.  **The logs show that:**  There is a notable pattern of a large number of TCP SYN requests originating from an unfamiliar IP address. These SYN requests are not followed by corresponding ACK responses, indicating an incomplete three-way handshake. The timing and volume of these requests align with the characteristics of a SYN flood attack.  **This event could be:**  Classified as a deliberate and malicious SYN flood attack. The evidence suggests a coordinated effort to disrupt the normal operation of the web server by exploiting the TCP handshake process, leading to service degradation and connection timeouts. |
|

|  |
| --- |
| **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.  Three-Way Handshake:  Step 1 - SYN (Synchronize):  The client initiates the connection by sending a TCP SYN packet to the server, indicating its intention to establish a connection.  Step 2 - SYN-ACK (Synchronize-Acknowledge):  The server responds with a TCP SYN-ACK packet, acknowledging the client's request and indicating its readiness to establish a connection.  Step 3 - ACK (Acknowledge):  The client sends an ACK packet back to the server, confirming the establishment of the connection. At this point, both parties can exchange data.  Malicious Actor Sending a Large Number of SYN Packets:  In a SYN flood attack, a malicious actor sends a massive volume of TCP SYN packets to the target server without completing the three-way handshake (i.e., without sending the final ACK). This overwhelms the server with half-open connections, consuming its resources.  Logs Indication and Server Impact:  The logs indicate a high volume of TCP SYN packets from an unfamiliar IP address.  When the attacker sends SYN packets without completing the handshake, the server keeps waiting for the final ACK that never arrives.  As a result, numerous half-open connections are left in a pending state, tying up server resources.  The server's capacity to establish new, legitimate connections is compromised, leading to a slowdown in response time and, eventually, connection timeouts for genuine users.  The server becomes unable to handle the influx of connection requests, causing service degradation and impacting the website's functionality. |