# 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 targeting the web server.  The logs show that: A large number of TCP SYN requests coming from an unfamiliar IP address were directed at the web server, significantly beyond the typical traffic volume.  This event could be: An orchestrated attempt by a malicious actor to overwhelm the server resources and disrupt the normal operation of our website, thus denying service to legitimate users. |
|

|  |
| --- |
| **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. **SYN (Synchronize):** The client sends a TCP packet with the SYN (Synchronize) flag set to the server, indicating a request to establish a connection. 2. **SYN-ACK (Synchronize-Acknowledgment):** Upon receiving the SYN packet, the server responds with a TCP packet with both the SYN and ACK (Acknowledgment) flags set, acknowledging the request for a connection. 3. **ACK (Acknowledgment):** The client then sends an ACK (Acknowledgment) packet back to the server, confirming the establishment of the connection.   Explain what happens when a malicious actor sends a large number of SYN packets all at once:  When a malicious actor sends a large number of SYN packets all at once, it overwhelms the server's resources as it tries to respond to each of these requests with a SYN-ACK and waits for the corresponding ACK which never comes. This hoards the server's resources causing it to become unresponsive or slow to legitimate traffic.  Explain what the logs indicate and how that affects the server:  The logs indicate an abnormally large number of SYN requests from a singular IP address, suggesting a SYN flood attack. The server becomes overwhelmed trying to process these fake connection requests, which consumes its resources, rendering it unable to handle legitimate requests. This results in the connection timeout errors observed when trying to access the company’s website, affecting both employees and potentially customers. |