# 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 is that the server cannot accommodate all the requests due to multiple requests being sent from a single IP address.  The TCP log shows that a single IP address keeps sending abnormal requests to the server every second. For the first 30 requests within 7 seconds, the server managed to grant access to requests from a legitimate employee. However, no requests were granted beyond that point.  This event could indicate a potential **DoS (Denial of Service) SYN flood attack**, where a large volume of requests from a single IP address overwhelms the web server. This overload causes the Transport layer of the TCP/IP model to malfunction. |
|

|  |
| --- |
| **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. Below are the steps involved:   1. **Synchronize (SYN) Request**: A connection request is sent from an employee to the web server. 2. **SYN-ACK Response**: The server responds with a Synchronize-Acknowledgement (SYN-ACK) to the employee. 3. **ACK (Acknowledgement)**: The employee sends an Acknowledgement (ACK) to complete the handshake.   When a malicious actor sends a large number of **SYN packets** simultaneously, it overwhelms the server, preventing it from completing the 3-way handshake with legitimate users.  The logs indicate that a **SYN flood attack** is underway, with someone sending consecutive SYN requests without allowing the server to respond to other requests, including those from the attacker. While the server managed to respond to the first 34 requests, no further handshakes were completed beyond that point, disrupting normal operations. |