# 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: DoS attack  The logs show that: the server stopped responding after being overloaded by numerous SYN packet requests.  This event could be: DoS attack 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. Explain the three steps of the handshake:   1. The client sends a SYN or synchronize request to the server. 2. The server will respond with a SYN/ACK packet to acknowledge the receipt of the device's request and establish the connection. 3. Once the server receives the final ACK packet from the device, a TCP connection is established   Explain what happens when a malicious actor sends a large number of SYN packets all at once: the web server stops responding to legitimate employee visitor traffic because there are no more sever source to access by the users.The visitors receive more error messages indicating that they cannot establish or maintain a connection to the web server.  Explain what the logs indicate and how that affects the server: the logs show that the server became overwhelmed and unstable to process the user’s SYN request. The server will lose its ability to open new access to user who receive timeout error message |