# 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 DoS attack is happening.  The logs show that: A large amount of SYN requests is reaching the server, coming from one single IP address and it is making the server unable to process additional connections, causing the website to be inaccessible.  This event could be: a non-distributed 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 connecting client device initiates the TCP handshake by sending a SYN packet. 2. The server receives SYN packet and sends SYN/ACK packet, leaving a port open to finalize the handshake processes. 3. The connecting client sends an ACK package, which the server receives, finalizing the handshake process.   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 in a short duration, the server cannot process all of them, and thus slows down or downright crashes.  Explain what the logs indicate and how that affects the server: the logs indicate a malicious actor is trying to take the website off air by flooding the server’s IP address with many SYN packets in a short period of time. This attack is a non-distributed DoS attack because all of the malicious packets come from the same IP address.  This network may be secured by configuring the firewall such that it blocks incoming connections from an IP address that sends too many packets within a determined amount of time. |