# 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:   * IT is a DoS attack   The logs show that:   * Server is not responding as it is overloaded with SYN requests   This event could be:   * The attack SYN flooding. | |
|

| **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 request is sent from client to the server  2. Destination server replies with the SYN-ACK packet  3.now client sends one last ACK request to connect  Explain what happens when a malicious actor sends a large number of SYN packets all at once:  Due to large number of SYN packets server gets overloaded and becomes unable to function properly  Explain what the logs indicate and how that affects the server:  -Log message indicates that the server is now unable to make any new connections and it is unable to process any SYN requests right now. |