# 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 DoS attack. The logs show that the server stopped responding after many SYN requests, which overwhelmed the server. This event could be caused by a 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. The three steps of the handshake are:   1. The user sends a SYN packet to the destination server to initiate connection. 2. The server sends back a SYN-ACK packet to signal that the connection can be established, acknowledging the source request. 3. The source finally sends an ACK packet which represents that the connection is established, recognizing the permission to connect.   A SYN flood attack occurs when a malicious actor sends so many SYN packets that the destination server cannot keep up with, and the result is the server shutting down.  The logs show that the server was responding correctly initially, it also established a TCP connection with the malicious actor, who then overwhelmed the server with many SYN packets, which caused the server to respond slower and slower to legitimate users until it stopped responding completely. |