# 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 possible reason for the website's connection timeout error is a DoS attack. The logs indicate that the web server becomes unresponsive when bombarded with SYN packet requests. This situation may point to a specific type of DoS attack known as 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. A SYN packet is sent from the source to the destination to initiate a connection. 2. The destination responds to the source with a SYN-ACK packet, approving the connection request and reserving resources for the source. 3. The source sends a final ACK packet to the destination, confirming acceptance of the connection.   Explain what happens when a malicious actor sends a large number of SYN packets all at once:  During a SYN flood attack, a malicious actor floods the server with a massive volume of SYN packets simultaneously, which exhausts the server's resources reserved for connection establishment. As a result, there are insufficient server resources available for legitimate TCP connection requests.  Explain what the logs indicate and how that affects the server:  The logs show that the web server has been overloaded and cannot process the incoming SYN requests from visitors. Consequently, the server fails to establish new connections, leading to connection timeout messages for those users. |