# 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 DDoS attack might be happening  The logs show that:  The server is overloaded with SYN packet requests.  This event could be:  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 to destination, requesting access.**  **2. The destination replies with a SYN-ACK packet, this way accepting the request. This will be used by the source to connect.**  **3. A ACK packet is sent from the source to the destination, acknowledging the permissions to connect.**  Explain what happens when a malicious actor sends a large number of SYN packets all at once:  **This will overwhelm the server, using all of its resources. When a legitimate request will be sent, it will not pe able to handle it.**  Explain what the logs indicate and how that affects the server: **The logs indicate that the web server has become overwhelmed and is unable**  **to process the visitors’ SYN requests.** |