# 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 Denial-of-Service attack.  The logs show that: The web server stops responding after being overwhelmed with many SYN packets requests.  This event could be: The consequence of 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. Explain the three steps of the handshake:   1. The SYN packet is sent from the device requesting to connect to the destination device. 2. The destination device replies to the source device with a SYN-ACK packet to accept the connection request. The destination will reserve resources for the final step of the handshake. 3. A final ACK packet is sent from the source device to the destination device acknowledging the permission to connect.   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 all at once, it overwhelms the available resources of the server to reserve for a connection. When this happens, there are no server resources left for legitimate TCP connection requests.  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. The server is unable to open a new connection to new visitors who receive a connection timeout message. |