# 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: DoS attack  The logs show that: the web server stops responding after it is overloaded with SYN requests.  This event could be:direct DoS 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.syn packet is sent frm device to server  2. The server responds with syn-ack to accept connection request  3.ack packet is sent from device to server to accept connection request  Explain what happens when a malicious actor sends a large number of SYN packets all at once: the web server stops responding after it is overloaded with SYN packet requests.  So the server isnt able to respond to visitors requests  Explain what the logs indicate and how that affects the server: the web server stops responding after it is overloaded with SYN packet requests. |