# 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:  The logs show that: There is a volume of incoming traffic and is losing its ability to respond to the abnormally large number of SYN requests.  This event could be:This could be a malicious attack purposely for DDOS |
|

|  |
| --- |
| **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 requesting to connect  2. A syn -ack is sent back form the connection destination back to the source to accept  3.The source accepts and sends a ACK accepting and acknowledging to connect .  Explain what happens when a malicious actor sends a large number of SYN packets all at once:  In this scenario . A lot of syn packets are sent to the destination . This overwhelms the server and it begins to malfunction . When this happens there are no longer connections available for tcp requests  Explain what the logs indicate and how that affects the server: The log shows the the server has been overloaded with lots of syn packets thereby causing it to be overwhelmed and there are not available server resources for the tcp requests. |