# 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 requests are overloading the web server with SYN packet requests.  This event could be: SYN Flooding, which is a form of a DoS 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. A SYN packet is sent from the source to the destination as a form of requesting to connect. 2. The destination then replies to the source with a SYN-ACK packet to accept this connection request. The destination then reserves resources for the source to connect. 3. A final ACK packet is sent from the source to the destination acknowledging permission granted to connect.   Explain what happens when a malicious actor sends a large number of SYN packets all at once: this overwhelms the server’s available resources to reserve resources for connections. Ultimately, this forces all resources to be reserved, which prevents any bandwidth for any legitimate traffic.  Explain what the logs indicate and how that affects the server: the logs showed that due to the server being overwhelmed, all visitor’s SYN requests were being unable to connect resulting in a connection timeout message. |