# 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: If the web server takes too long to respond, the gateway server produces a timeout error message to the requesting browser  The logs show that: After an attacker’s SYN is answered normally , he keeps on sending SYN requests for which the system starts to struggle and after an abnormal amount of SYN requests the web server stops responding.  This event could be: A type of DOS attack called SYN Flood attack that usually keeps on sending SYN request to the web server in a three-way handshake process. | |
|

| **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.First, a SYN request is sent to the web server to form a connection with a web page  2. The [SYN,ACK] is the web server’s response to the visitor’s request for the connection  3.The ACK packet from the visitor acknowledges the permission to connect and the connection is thus established.  Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a large number of SYN request are sent, the server works for other normal visitors at first, but as the SYN request are sent at an abnormal amount the server starts to struggle and error appears and finally the server stop responding.  Explain what the logs indicate and how that affects the server: The logs indicate that the server is overwhelmed with the SYN requests and is unable to form an connection to any visitors. |