# 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: A malicious threat actor is sending multiple SYN requests to the server and the server is getting overloaded with these requests unable to deal with these many requests.  This event could be: from the log data, it is very clear that this is a SYN flood attack by an external threat actor trying to flood the server with a huge number of SYN requests. | |
|

| **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 user machine sends a SYN request to the server to initiate the three-way handshake. 2. Once the SYN request is received by the server and processed, a SYN-ACK request is sent back to the user’s address suggesting to form a connection between server and client. 3. After receiving acknowledgement from the server side, the client machine sends the final ACK request giving permission to the server to form the connection for further transmission of data.   Explain what happens when a malicious actor sends a large number of SYN packets all at once: the server machine tries to process all the requests one by one and respond to them by sending a SYN-ACK request. But due to the large number of SYN packets, the server gets overwhelmed and is unable to keep up with the incoming packets. Leading to an unresponsive server.  Explain what the logs indicate and how that affects the server: from the log data, it is very clear that this is a SYN flood attack by an external threat actor trying to flood the server with a huge number of SYN requests. The threat actor is sending various SYN packets every second. Due to this server has become unresponsive and hence the client machines receive an gateway error. |