# 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 SYN request from the same IP address multiple times in a second.**  The logs show that: **Repeated SYN requests from a specific ip address mixed in with legitimate connections from customers.**  This event could be: **A SYN request 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. **Firstly, a SYN or syncronize request is sent to the TCP server.**  2. **The TCP server sends back a SYN/ACK or syncronize/acknowledgement response to the client.**  3. **Lastly, the client sends back it’s own ACK response and TCP connection is established.**  Explain what happens when a malicious actor sends a large number of SYN packets all at once: **When a malicious actor sends a large number of SYN requests to a TCP server, the server cannot satisfy all requests in such quick sucession.**  Explain what the logs indicate and how that affects the server: **The logs indicate that a single IP address is sending an abundance of SYN requests to the TCP server. This affects the server by flooding all of the ports so that legitimate requests cannot be fulfilled and malicious requests overload all available ports.** |