# 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 DDoS Syn Attack. A hacker is sending a multiple SYN flood to the TCP to disrupt the TCP.  The logs show that at first, the TCP is working normal when an employee attempts to access a website. Then, on log 70, the server begins to experience the first signs of an overload. This event could be the result of a DDos attack called SYN Flooding. | |
|

| **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. When a client requests to access a website, they initiate the handshake by sending a SYN (synchronize) packet to the server.   2. Once the packet is received by the server, the server acknowledges the SYN packet and sends out a SYN-ACK to the client.  3. ONce the client receives the SYN\_ACK packet, it responds with an ACK to confirm the connection.  When a malicious actor sends a large number of SYN packets all at once, the server overloads and eventually crashes. It is hard for the server to process the incoming SYN packet requests. This can result in a time our error or a RST,ACK packet as well.  Explain what the logs indicate and how that affects the server: The logs suggest that after so many SYN packet requests, the server stops responding to legitimate web browsing attempts. This becomes an issue because customers trying to access the DNS continuously get an error message. |