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 DoS attack

The logs show that web server unresponsive after being flooded with SYN requests

This event could be a SYN 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.

1. SYN (source → destination)
2. SYN/ACK (destination → source)
3. ACK (source → destination)

When a malicious actor sends a large number of SYN packets all at once:
Servers are overwhelmed and no resources are left for further TCP connections

Logs at first show normal TCP connection flow, then port number 54770 also starts with a normal TCP connection but then floods the server with SYN requests, overwhelming the server and it becomes unable to process further SYN requests and cannot form a TCP connection with new visitors as well.