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: it could a malicious threat actor or a server side issue

The logs show that: one IP address has been flooding the server with SYN packet 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. Explain the three steps of the handshake:
1. The SYN packet is the initial request to the server

2. A SYN,ACK packet is the servers response to the visitors request agreeing to the connection

3. An ACK packet is the visiting machines acceptance for a connection

Explain what happens when a malicious actor sends a large number of SYN packets all at once: With a large number of SYN packets being sent, it overwhelms the server and slows down service for everyone

Explain what the logs indicate and how that affects the server:The logs indicate that a singular IP address has been flooding the network with SYN packets which has completely shut the server down