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: Malicious actor is targeting the web server

The logs show that: There are large amounts of TCP SYN requests flooding the server

This event could be: 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. The client sends a request to the web server. This is the SYN packet. From source to destination

2. The server receives the request from the client. It replies with a SYN/ACK to accept the incoming request.

3. The last ACK is sent from the source to acknowledge the permission to connect to the server

Explain what happens when a malicious actor sends a large number of SYN packets all at once:
When the client sends a lot of SYN packets at once, the server gets overwhelmed. This is a SYN flooding attack, and causes a denial of service for anyone using the web server.

Explain what the logs indicate and how that affects the server: Logs indicate that the server is overwhelmed and it can’t process legitimate syn requests. Server is unable to open a new connection for those waiting.