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: overloading of the server

The logs show that: there is a large amount of incoming SYN packets on the network

This event could be: a potential SYN DoS attack by a threat actor who is trying to flood the server with SYN packets

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. Source sends SYN packet to the server to establish a connection

2. Server sends back SYN/ACK packet to the source to acknowledge the connection that is trying to establish the connection

3. Upon receiving SYN/ACK from the server, the source sends ACK packet back to the server to complete the three-way handshake require to establish a conection

Explain what happens when a malicious actor sends a large number of SYN packets all at once:

If the malicious actor sends a large number of SYN packets all at once, the server gets overload with connection requests as it runs out of available ports to establish a connection which causes it to crash or stop reponding to further requests

Explain what the logs indicate and how that affects the server:
The logs indicates that there was unusual surge in unwanted traffic on the network. There were a large amount of incoming requests on the server within a short time period. The amount of requests on the network exceeded the available ports which led to overloading of the server and causing it to stop responding.