# 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: Dos (Denial of Service) Attack.

The logs show that: Potential malicious actor with IP address (203.0.113.0) sent multiple SYN packets to the company server (192.0.2.1) which appears to have overloaded the server.

This event could be: 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. Client initiates a connection to a server by sending the SYN flag set to 1.

2. The server responds by sending the SYN and ACK flags set to 1.

3. The client sends the ACK flag set to 1

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When multiple SYN packets were sent to the server, the increased traffic diverted resources away from the server. The increased resources needed to process the SYN packets eventually caused the server to stop responding to normal traffic.

Explain what the logs indicate and how that affects the server: The logs indicate multiple SYN packets being sent from IPv2 address 203.0.113. The server responded to the SYN packets normally, however, 203.0.113 continued to send several more within a short period of time. The logs show the server stopped responding to all requests after log line 80.