# 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 that the logs show that one particular IP address (203.0.113.0) has flooded the server with SYN packet requests, which is greater than the server resources available to handle the requests. Hence why the server is overwhelmed and unable to respond to the requests. This is a DoS direct attack, since it originates from a single source.

This event could be a DoS SYN flood Attack, because it flooded the server with SYN packet requests.

## 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. The handshake consists of 3 steps:
1. SYN = The [SYN] packet is the initial request from an employee visitor trying to connect to a web page hosted on the web server. SYN stands for “synchronize.”

2. SYN/ACK = The [SYN, ACK] packet is the web server’s response to the visitor’s request agreeing to the connection. The server will reserve system resources for the final step of the handshake. SYN, ACK stands for “synchronize acknowledge.”

3.ACK = The [ACK] packet is the visitor’s machine acknowledging the permission to connect. This is the final step required to make a successful TCP connection. ACK stands for “acknowledge.”

For a SYN flood attack to happen, a malicious actor will send a large number of SYN packets all at once, which will flood the server and overwhelms it with the unusual number of requests that it cannot accommodate, therefore the server will stop responding.

The rows highlighted and labeled yellow are failed communications between legitimate employee website visitors and the web server.

The logs indicated that the web server has become overwhelmed and unable to process the new visitors’ SYN requests. The visitor will receive a timeout error message in their browser and the connection attempt is dropped.