# 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:
The web server is receiving an unusually large number of requests that it cannot handle, causing legitimate users to be unable to connect.

The logs show that:

- One IP address (203.0.113.0) repeatedly sends TCP SYN packets to the web server.
- The server responds with SYN-ACK, but the attacker does not complete the connection with an ACK.
- Normal user traffic is either slowed down or receives timeout errors (504 Gateway Time-out).

This event could be:
A SYN flood attack, which is a type of Denial of Service (DoS) attack aimed at overwhelming the server with half-open TCP connections.

## Section 2: Explain how the attack is causing the website to malfunction

Three steps of a normal TCP three-way handshake:

1. SYN – The client sends a request to the server saying, “I want to connect.”
2. SYN-ACK – The server responds, saying, “Okay, I’m ready for you.”
3. ACK – The client replies, “Great, the connection is established,” and communication begins.

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

- The server responds to each SYN with a SYN-ACK and allocates resources for the connection.

- The attacker never sends the final ACK, leaving the connections half-open.
- As more and more SYN packets arrive, the server's connection table fills up, preventing legitimate users from connecting.

What the logs indicate and how that affects the server:

- The Wireshark logs show hundreds of SYN packets from 203.0.113.0 with no ACKs following.
- Normal users (198.51.100.x) eventually receive timeouts or HTTP 504 errors because the server cannot accept new connections.
- The attack overloads the server and causes the website to become unresponsive until the traffic is mitigated.