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 takes too long to respond.**

The logs show that: **web server is having to keep up with the abnormal number of SYN requests coming in at a rapid pace**

This event could be: **SYN flood attack which is a type of DoS 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. **SYN - Initial request from a visitor trying to connect to a web page hosted on the web server.**

2. **SYN/ACK - Is the web server's response to the visitor's request agreeing to the connection.**

3. **ACK - Visitor's machine acknowledging the permission to connect.**

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

The web server will get overwhelmed with the number of requests and will stop responding.

Explain what the logs indicate and how that affects the server: **The web server stops responding to legitimate employees visitor traffic. The visitors receive more error messages indicating that they cannot establish or maintain a connection to the web server. The IP address that is attacking the web server from the log seems to be from 203.0.113.0**