# 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:** SYN flood attack

**The logs show that:** The Wireshark TCP log section started at log entry number (No.) 47, indicating 47 messages were sent and received by the web server in 3.1 seconds. Further, sending packets between IP 198.51.100.0/24 (employees' computers) and IP 192.0.2.1 (company's web server) was influenced with malicious IP 203.0.113.0.

**This event could be:** As there is only one IP address attacking the web server, it can be assumed this is a direct DoS 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. SYN (Synchronize) - The client initiates the connection by sending a SYN packet to the server. This packet informs the server that the client wishes to establish a connection.
2. SYN-ACK (Synchronize-Acknowledge) - Upon receiving the SYN packet, the server responds with a SYN-ACK packet. This packet acknowledges the client's SYN packet and also contains the server's own SYN message to initiate its sequence number count.
3. ACK (Acknowledge) - The client responds to the server's SYN-ACK packet with an ACK packet. This completes the handshake, confirming the establishment of a bidirectional TCP communication channel.

**Explain what happens when a malicious actor sends a large number of SYN packets all at once:** The attacker bombards the target server with many SYN packets. The server responds to each with a SYN-ACK, awaiting a final ACK to complete the three-way handshake. The attacker doesn't send the final ACK. The server's resources get tied up waiting for ACKs that never come, leading to potential overloads and service disruptions.

**Explain what the logs indicate and how that affects the server:** Initially, the attacker's SYN request is answered normally by the web server (log items 52-54). In the next 20 rows, the log begins to reflect the struggle the web server is having to keep up with the abnormal number of SYN requests. The rest of the log shows the web server stops responding to legitimate employee visitor traffic. The visitors receive more error messages indicating that they cannot establish or maintain a connection to the web server. From log item number 125 on, the web server stops responding. The only items logged at that point are from the attack.