Cybersecurity Incident Report

Section 1: Identify the type of attack

One potential explanation for the website's connection timeout error message is: Denial of Service (DoS) attack

The logs show that:
Multiple SYN requests from the same IP

This event could be:
SYN Flood Attack

Section 2: 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:

Step 1: SYN Request is sent to a web server requesting acknowledgment for connection from the client.

Step 2: Server Accepts the request and sends [SYN, ACK] to the client in return.

Step 3: Acknowledgement [ACK] is sent to the web server to confirm that the connection is established.

In the case of a SYN flood attack, a malicious actor sends an excessive number of SYN packets simultaneously. The web server becomes overwhelmed, busy accepting the synchronization requests from the attacking IP address, "203.0.113.0." At a certain point, the server stops accepting any other requests from genuine IPs. Ultimately, the web server stops responding, causing the observed network interruption.

The logs from Wireshark confirm that IP "203.0.113.0" is the attacker repeatedly requesting synchronization from the web server, IP "192.0.2.1," leading to server flooding and the subsequent unresponsiveness to legitimate incoming

requests.