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 server has run out of space. The logs show that: **There are a large number of TCP [SYN] requests being made at port 443 from an unknown IP address.** This event could be: Potential SYN flood attack; a type of DoS attack that simulates a TCP/IP connection & floods a server with SYN packets.

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: **1.The synchronize [SYN] packet is the initial request trying to connect a web page hosted on a web server** **2. The synchronize/ acknowledge [SYN/ACK] packet is the web servers response to the visitor's request agreeing to the connection. The web server then reserves space for the third step of the handshake.** **3. The acknowledge [ACK] packet is the visitor's machine acknowledging permission to connect, which is the final step required to make a TCP/IP connection successfully.** **Once the server has received a [SYN] packet, it responds to the visitor by sending [SYN/ACK] packets whilst also reserving space on the server to receive the final [ACK] packet from the visitor. If you multiply this exponentially in a brief duration of time, the processor of the server will quickly slow down to send [SYN/ACK] packets back to the malicious actor while also reserving space on the server itself to receive the malicious actor's expected [ACK] packets, whilst also trying to process any legitimate requests made by users.** **The Logs indicate that many [SYN] requests are being made to the server at port 443 by unknown IP address 203.0.113.0. Legitimate requests are made to the server via port 443 and are being delayed. Port 443 is designated specifically for HTTPS traffic (traffic secured by encryption.) While handling legitimate requests, the server is responding with [SYN/ACK] packets to the unknown IP, which is slowing down the legitimate requests by reserving space on the server for [ACK] packets expected in response by the unknown IP. The unknown IP is not responding with [ACK] packets, which has caused the server to send reset/ acknowledge [RST/ACK] packets to all users. Since the server no longer has space to receive [ACK] from users, the gateway has timed out. The server has sent a timeout packet to the legitimate users and continues to receive [SYN] packets from the unknown IP which can no longer reserve space to send [SYN/ACK] or receive [ACK] packets from any user.**