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 a DoS attack. The possible attack is the direct SYN flooding attack where a TCP connection is simulated and the server is flooded with SYN packets. This is due to the fact that there is only one IP address overloading the server with SYN packet requests.

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. The visitor sends out a SYN request, the web server then responds to the request with a SYN/ACK request, the visitor then responds with an ACK packet Due to the malicious actor sending out a large number of SYN packets all at once, the web server ran out of resources available to handle the requests. The server then became overwhelmed and unable to respond to the requests. The log indicates that the server was flooded by the SYN request from 203.0.113.0 which means the server was attacked by SYN flooding. Due to this, the server cannot establish and maintain a connection to the visitors so they cannot access any of the webpage. This attack could cost a lot of money and time to rebuild the infrastructure of the network. Potential ways to secure the network so this attack can be prevented in the future is to use NGFWs to monitor suspicious traffics and to set a limited amount of requests that can be made from a specific IPs so a direct DoS attack cannot be made.