Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
The company's web server is flooded by SYN request from the same IP address 203.0.113.0. This event could be a TCP 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. The client want to establish connection with the server and sends a SYN request to start communication. 2. The server responds by sending a SYN-ACK to the client 3. In the final part client sends a ACK acknowledges the response from the server to establish a reliable connection, When the server receives more number of SYN request than it can handle it overwhelms the server ability to provide resources for connection The log shows that the server has been flooded with SYN request from one IP address that overwhelmed the server and hence could not provide connected to the user and hence a time out message is given to the user.