Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
The company's website traffic is flooded with SYN requests on the 443 port and is unresponsive. The logs show that the source IP 203.0.113.0 No. 7-9 establishes a successful connection, later the IP sends floods of SYN requests between No. 12-175. This event could be a possible SYN DoS attack on the company's website.

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 first part of the handshake is a "synchronize" or SYN request that is sent from the client to the web server [SYN]. 2. The second part of the handshake is the web server's acknowledgment to the request or [SYN, ACK], ACK. 3.The last part is the client's acknowledgement of the approval from the web server, [ACK]. When malicious actors send a flood of SYN request attacks, it causes the server to overload with the traffic requests and the server no longer has the resources to handle them. The logs indicate that the malicious actor 203.0.113.0 flooded the web server on port 443 with SYN requests, causing the server to timeout due to lack of resources. The attack caused the company financial costs, customer reputation as well as company operational time.