Cybersecurity Incident Report

Summary of the Problem
Users are getting a “Connection timeout” message on the company website. Using a packet sniffer to capture data packets to and from the server, there is a large amount of requests that is overwhelming the server.

Analysis
A DoS attack is when the network is flooded with requests in attempts to crash the server. In this case, this would be a SYN flood where the requests are SYN requests. There are three steps to establishing an initial connection (1. SYN, 2 SYN-ACK, 3. ACK) SYN flood most likely is the case here because of the IP address being used from the same location over and over. The IP that the attack was coming from was 203.0.113.0 The attacker is rapidly sending SYN requests and flooding the server without completing the connection. This is consuming the server’s resources while it waits for a response from the connection, causing the response times to get longer and longer. As it is tied up waiting for a response, more requests are sent for the network to try to respond to. Once the system got overwhelmed the only requests coming through were the SYN requests from 203.0.113.0. Because the system is backed up with these requests, it is not able to process the SYN requests of other visitors and is giving them the connection timeout error message.