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 that the firewall was misconfigured and is blocking all requests or the server is being overwhelmed with a large number of requests which could be caused by a Denial of Service attack. The logs show that there were a large number of SYN requests from the source IP 203.0.113.0 and the server couldn't respond to all of them.This event could be a form of Denial of Service attack known as a SYN flood attack where the malicious actor sends a large number of SYN packets which causes the server to be overwhelmed and unable to respond to other connection requests sent by legitimate users to use the site.

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.In a normal case it should occur as follow: 1- The client sends a SYN packet to the server to indicate the start of the connection. 2- The server sends back a SYN-ACK packet to indicate that the server has received the connection request and is ready to form a connection. 3- The client sends an ACK packet back to the server to confirm the receipt of the server's SYN-ACK. A malicious actor can exploit this three-way handshake by performing a SYN flood attack which is a type of Denial of Service (DoS) attack where the malicious actor sends a large number of SYN packets which causes the server to be overwhelmed and unable to respond to other connection requests sent by legitimate users to use the site. This could clearly be seen in the logs where at first the server was able to respond normally to the requests but when the threat actor performed the SYN flood attack the server was no longer able to respond to other requests and the server was slowed down.