Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
One potential cause for the problem with the webserver is a denial of service SYN flood attack. In review of the network logs there are a large number of SYN requests to the webserver originating from IP 203.0.113.0. These requests are causing the webserver to become overloaded and unable to respond.

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 three steps of this handshake are: 1. First the sending device sends a SYN request to the server. 2. The server will acknowledge the request with [SYN, ACK] 3. Finally an acknowledgment of the connection is sent back to the server from the originating device with the message [ACK] When a device sends a massive number of SYN requests to the server eventually the server will no longer be able to respond to all the requests and will become overloaded causing the server to no longer be able to respond to requests. In this case we are seeing what would be considered a SYN flood DOS attack as the server is receiving an overwhelming number of SYN requests from a single IP address.