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: The IP address 203.0.113.0 keeps sending at least 3 SYN request packets each second. The logs show that: The IP address 203.0.113.0 keeps sending at least 3 SYN request packets each second. It blocks the other IP addresses from sending SYN request packets and interrupts established connections. This event could be: A direct DoS SYN attack on the company's web server.

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 source IP address sends a SYN request packet for connection to the destination web server. 2. The destination web server receives the request and decides to acknowledge or reject it. If acknowledged it will send back the source IP address a SYN ACK packet. 3. An ACK packet and connection to the server are sent back to the source IP address. Explain what happens when a malicious actor sends a large number of SYN packets all at once: It floods the server with SYN request packets that can block potential valid users' SYN request packers and connections to the server. Explain what the logs indicate and how that affects the server: The logs indicate that IP address 203.0.113.0 floods the web server with SYN request packets. The packets overwhelm the server and block any valid SYN request packets and connections to the server. The server would send back a RST/ACK packet to valid IP addresses.