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: a DoS attack. The logs show that: there are a copious amount of SYN packet requests originating from IP address 203.0.113.0. This event could be: SYN Flood attack, which is a type of DoS attack.

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. A SYN packet is sent from the source to the destination, attempting to establish a connection. 2. The destination replies with a SYN-ACK packet back to the source to accept the connection request. The destination will reserve resources for the connection. 3. The source sends an ACK packet to the destination allowing permission for the connection. Explain what happens when a malicious actor sends a large number of SYN packets all at once: During a SYN flood attack, the server is overwhelmed and cannot reserve resources to establish a connection. Without resources, a TCP connection cannot be made. Explain what the logs indicate and how that affects the server: The company’s server IP address is 192.0.2.1 and all company employees have IP addresses within the range of 198.51.100.0/24. The logs show that a mystery IP address (203.0.113.0) is spamming the company server with SYN packet requests, and even when the server replies with a SYN-ACK packet, the malicious actor continues to send SYN packets. Due to the massive amounts of ‘fake’ SYN packets coming from the malicious actor, the server cannot handle actual SYN packet requests from the company’s employees. Therefore, the employees will receive a timeout error message.