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: DoS attack, specifically a SYN Flood attack. The logs show that: A single source IP Address ‘203.0.113.0’ is sending an abnormal and continuous volume of TCP packets with the ‘SYN’ flag to the company’s web server ‘192.0.2.1’. This event could be: DoS SYN Flood 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. SYN: The client sends a ‘SYN’ packet to the server to initiate a connection. 2. SYN, ACK: The server responds with a ‘SYN, ACK’ packet, confirming receipt of the request and allocating resources for the new connection. 3. ACK: The client finalizes the process by sending a ‘ACK’ packet back to the server, thereby establishing the connection. Explain what happens when a malicious actor sends a large number of SYN packets all at once: half-open connections, which exhausts its system resources. Once its resources are depleted, the server becomes overwhelmed and is unable to respond to new requests from legitimate users, causing a DoS. Explain what the logs indicate and how that affects the server: The logs show that a single attacker IP address ‘203.0.113.0’ is continuously sending ‘SYN’ packets to the company’s web server. This flood of requests overwhelms the server, which begins to struggle the traffic. As a result, legitimate users are denied service.