Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
One plausible explanation for the website's connection timeout issue is a **SYN flood attack**, a subset of Denial of Service (DoS) attacks. The logs reveal an abnormal influx of SYN packet requests from the malicious IP address 203.0.113.0. These excessive requests prevent the server from responding effectively to legitimate traffic, leading to service unavailability for users.

Section 2: Explain how the attack is causing the website malfunction
When website visitors attempt to connect to the server, the connection is established through a three-step TCP handshake: 1. The visitor's system sends a SYN packet to initiate the connection. 2. The server responds with a SYN-ACK packet, confirming receipt and reserving resources for the connection. 3. The visitor's system completes the handshake by sending an ACK packet to finalize the connection. In a SYN flood attack, a malicious actor overwhelms the server by sending a high volume of SYN packets without completing the handshake. This forces the server to reserve resources for incomplete connections, rapidly exhausting its capacity to handle new, legitimate requests. The logs demonstrate that the server struggled to manage legitimate connections, with users receiving connection timeout errors due to the lack of available resources. This attack disrupted normal operations, causing downtime and impacting the organization's ability to serve its customers effectively.