# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this network interruption** |
| --- |
| The connection timeout error message on the website suggests a potential cause: a flood of SYN requests originating from an external source. The logs reveal a significant number of SYN requests originating from the same IP address in a very short period, specifically from IP address 203.0.113.0. This pattern indicates a direct DoS SYN flood attack, where the attacker floods the server with numerous connection requests to overwhelm its resources, leading to service disruption or denial for legitimate users. |

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| A three-way handshake using the TCP protocol occurs when website visitors attempt to connect to a web server. Firstly, the visitor sends a [SYN] packet, synchronizing its intent to connect. Secondly, the server responds with a [SYN, ACK] packet, agreeing to the connection and reserving resources. Finally, the visitor sends a [ACK] packet, acknowledging the server's permission and completing the handshake. However, when a malicious actor sends many SYN packets simultaneously, it floods the system, overwhelming it with connection requests. This flood disrupts the website, causing it to go down or consume excessive memory, rendering it unusable for genuine users. While the site may initially handle the flood and accept SYN requests from legitimate users, logs indicate a rapid degradation in response time due to the overwhelming volume of requests, impacting the server's performance and ability to serve genuine users effectively. |