# 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: **SYN Flood Attack**  The logs show that:   * There is a high volume of SYN packets being sent from the IP address **203.0.113.0** to the server at **192.0.2.1**. * The server responds with SYN-ACK packets, but the client (attacker) does not complete the three-way handshake by sending the final ACK packet. * The server is overwhelmed by the large number of half-open connections, leading to resource exhaustion.   This event could be:   * A **Denial of Service (DoS)** attack, specifically a **SYN Flood**, where the attacker exploits the TCP three-way handshake process to overwhelm the server with incomplete connection requests. | |
|

| **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 request to start a connection. 2. **SYN-ACK**: The server acknowledges the request and agrees to connect. 3. **ACK**: The client confirms, and the connection is established.   Explain what happens when a malicious actor sends a large number of SYN packets all at once:   * The server allocates resources to each incoming SYN request, expecting to complete the three-way handshake. * Since the attacker does not send the final ACK, the server's resources are tied up, preventing legitimate users from establishing connections. * Eventually, the server becomes overwhelmed and may stop responding to legitimate requests, leading to a **connection timeout error** for users trying to access the website.   Explain what the logs indicate and how that affects the server:   * The logs show a high volume of SYN packets from the IP address **203.0.113.0**, but no corresponding ACK packets to complete the handshake. * The server is forced to allocate resources to these incomplete connections, leading to resource exhaustion. * As a result, legitimate users experience slow loading times or are unable to access the website, resulting in a **denial of service**. |