# 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:** The web server was overwhelmed by a flood of incomplete connection requests, which exhausted its resources and prevented it from responding to legitimate users. This resulted in connection timeout errors for anyone attempting to access the website, including employees.  **The logs show that:** There was an abnormally high number of TCP SYN requests originating from a single unfamiliar IP address (203.0.113.0). These requests did not follow through with the final steps of the TCP handshake, leaving many half-open connections. This pattern is consistent with a TCP SYN flood attack.  **This event could be:** A **Denial of Service (DoS) attack**, specifically a **TCP SYN flood**. In this type of attack, an attacker exploits the TCP handshake process by sending numerous SYN requests without completing the connection, ultimately overwhelming the server and disrupting service availability. | |
|

| **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 (Synchronize):** The client sends a SYN packet to the server to initiate a new TCP connection and indicate the client's initial sequence number. 2. **SYN-ACK (Synchronize-Acknowledge):** The server responds with a SYN-ACK packet to acknowledge the request and provide its own initial sequence number. 3. **ACK (Acknowledge):** The client replies with an ACK packet, confirming the receipt of the server’s SYN-ACK. Once this step is complete, the connection is fully established and data transfer can begin.   **Explain what happens when a malicious actor sends a large number of SYN packets all at once:** When an attacker floods the server with a high volume of SYN packets without completing the handshake, the server allocates memory and keeps these connections in a half-open state. Because the final ACK never arrives, these incomplete connections consume resources. If the number becomes too high, the server runs out of space to accept new connections, preventing legitimate users from connecting and causing the server to become unresponsive.  **Explain what the logs indicate and how that affects the server:** The logs show a large number of SYN packets originating from the same unfamiliar IP address (203.0.113.0) with no corresponding ACKs. This pattern indicates a **TCP SYN flood** attack. The server, overwhelmed by the volume of half-open connections, is unable to respond to legitimate traffic. This causes the website to time out and appear offline to employees and customers trying to access it. |