# 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:   * A SYN flood attack, a form of Denial-of-Service (DoS) attack.   The logs show that:   * There is a repetitive pattern of SYN packets being sent from the IP address 203.0.113.0 to the company's web server without corresponding ACK responses.   This event could be:   * A malicious actor attempting to exhaust the server's resources by continuously sending SYN packets without completing the three-way handshake, thereby causing legitimate traffic to be denied or delayed in service. |
|

|  |
| --- |
| **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 request a connection.   2. SYN, ACK: The server acknowledges the client's SYN packet by sending a SYN, ACK packet back to the client. This also indicates the server's willingness to establish a connection.  3. The client acknowledges the server's SYN, ACK packet, completing the three-way handshake and establishing the connection.    Explain what happens when a malicious actor sends a large number of SYN packets all at once:   * The server becomes overwhelmed attempting to reserve resources for each of these incomplete connection requests. This can exhaust the server's available resources, making it difficult or impossible for legitimate traffic to establish connections.   Explain what the logs indicate and how that affects the server:   * The logs show that the IP address 203.0.113.0 is repetitively sending SYN packets to the server without completing the handshake. This continuous stream of SYN packets without corresponding ACKs suggests an intentional effort to flood the server, consuming its resources. * Over time, this can cause the server to slow down or become unresponsive, leading to the "connection timeout" errors experienced by legitimate users. |