# 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 DoS attack  The logs show that: One IP address, 203.0.113.0, is flooding the server with SYN packets  This event could be: A direct denial of service attack, SYN flood |
|

|  |
| --- |
| **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. The client sends a SYN packet to the server 2. The server acknowledges the SYN packet with an ACK packet 3. The client sends back another ACK packet and the session begins   Explain what happens when a malicious actor sends a large number of SYN packets all at once: The server wastes resources trying to respond to all of them, eventually running out of resources for legitimate traffic and crippling it.  Explain what the logs indicate and how that affects the server: The logs indicate the server has been flooded by SYN packets from a single IP address. The malicious IP address has sent no ACK packets back to the server after the initial handshake, indicating that the client is maliciously trying to flood the server with SYN packets. The server is dutifully responding to all the SYN packets with ACK packets, eventually running out of resources to respond to all of them. |