# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| One possible explanation for a site connection timeout error message is a DoS attack.Logs show that an abnormal number of SYN requests arrive at a rapid rate, sent requested by ip address 203.0.113.0. Making the web server stop responding.This event can be a direct DoS SYN flood attack. |
|

|  |
| --- |
| **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 - requesting connection 2. SYN/ACK - response of the web server to the visitor's request agreeing to the connection. The server will reserve system resources for the final handshake step 3. ACK - confirming the connection permission   Explain what happens when a malicious actor sends a large number of SYN packets all at once: It simulates a TCP connection and floods the server with SYN packets, which targets network bandwidth to decrease traffic. Causing the web server to fail by stopping responding to legitimate traffic  Explain what the logs indicate and how that affects the server: the web server stops responding to legitimate traffic from employee visitors. Visitors receive more error messages indicating that they are unable to establish or maintain a connection to the web server. |