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: Too much traffic or the server is overloaded. The logs show that: The server is receiving requests from 1 IP address. All other traffic is responding ok except for one request. This event could be: 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. device to send a SYN, or synchronize, request to the server 2. server responds with a SYN/ACK packet 3.Once the server receives the final ACK packet from the device, a TCP connection is established Explain what happens when a malicious actor sends a large number of SYN packets all at once: The request(s) is larger than the number of available ports on the server, then the server will be overwhelmed and become unable to function. Explain what the logs indicate and how that affects the server: Logs started showing An HTTP/1.1 504 Gateway Time-out, server will be overwhelmed and become unable to function.