Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
The website is experiencing timeout error for any user that tries to establish connection and complete teh tCP handshake. The log indicates hundreds of request form the same IP address initiating a TCP handshake by spamming SYN request, this has preclude other user from establishing connection to our website and receiving a timeout error because the server fails to complete all the handshakes required for a TCP connection. This event is likely a SYN Denial of service attack given that it is the same ip that has attempt to flood the server with SYN request.

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 first handshake, the client ask the server if it has any open connections 2. SYN ACK - If the server has open ports, it sends back a SYN-ACK packet that includes its SYN and the ACK number. The server also allocates resources for the connection and generates its own SYN sequence number. 3.ACK - The client sends a final ACK message Explain what happens when a malicious actor sends a large number of SYN packets all at once: The client request will get ignored because there are no open connections Explain what the logs indicate and how that affects the server: The log indicated that the attacker using IP address 192.0.2.1 has been requesting SYN handshake every 0.3 seconds or so and that has gradually cause the server to shut down any other request.