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: The abnormal amount of TCP SYN requests packets The logs show that: There is a malicious attacker that is most likely spoofing an IP address to flood the server with SYN packets. This event could be: A DoS attack, more specifically a 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: The client (the PC initiating the connection) sends a SYN (synchronize) packet to the server to request a connection. 2. SYN-ACK: The server receives the SYN and responds with a SYN-ACK packet, acknowledging the request and indicating readiness to establish a connection. 3. ACK: The client receives the SYN-ACK and responds with an ACK (acknowledgment) packet, completing the handshake. Explain what happens when a malicious actor sends a large number of SYN packets all at once: simulates a TCP connection and floods a server with SYN packets, shutting down or disrupting the servers ability to operate. Explain what the logs indicate and how that affects the server: The logs showed a huge volume of SYN packets from an unfamiliar IP address, signaling a possible SYN flood attack. This in turn, overwhelms the server and its ability to respond to any other request, as the logs shows how at first the server sends a few [RST, ACK] packets to the clients, signaling the inability to respond on time. However, then the malicious attacker finally overwhelms the server and all the logs show are the SYN packets from the IP 203.0.113.0, making the server give all the other visitors a timeout error message.