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: A DOS attack flooded by SYN requests The logs show that: One IP address sent a request for many SYN packets This event could be: a SYN DOS 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. The visitor's computer sends a SYN packet in an attempt to connect 2. The web server responds with a SYN ACK packet to approve the connection 3. The visitor's computer sends an ACK packet to confirm the connection Explain what happens when a malicious actor sends a large number of SYN packets all at once: When the malicious actor sends too many SYN packet requests, the server's resources are not large enough to handle all the traffic, and it will be unable to respond to all the requests. Explain what the logs indicate and how that affects the server: The logs indicate that one user sent a request for far too many SYN packets, and as a result, the system did not allow proper connection between legitimate employees and the server.