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 network level denial of service (DoS) attack, called a SYN flood attack, that targets network bandwidth to slow traffic. The logs show that: the web server stops responding to legitimate employee visitor traffic. This event could be: As there is only one IP address attacking the web server, you can assume this is 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 Client to server Initial Connection Request- SYN 2 Server Response SYN-ACK 3. Client Acknowledgment ACK Explain what happens when a malicious actor sends a large number of SYN packets all at once: No server resources available for TCP connection request Explain what the logs indicate and how that affects the server: The server is unable to open a new connection to new visitor