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 that the server has too many requests for connection. The logs show that there are many SYN requests for connecting to the server from a single IP address, which at first are being acknowledged and the server responds - however, later on, the server stops responding completely; an employee cannot connect to it. This event could be: A SYN flood 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. The three steps of the handshake are: 1. SYN - “synchronize” - an initial part of the handshake; a visitor of the web page sends a request to the web server in order to connect to it and access data. 2. SYN ACK - “synchronize and acknowledge” - ACK packet is the web server’s response to the visitor’s request agreeing to the connection. 3. ACK - “acknowledge” - a final step of the TCP handshake, this packet is sent from the visitor's machine acknowledging a permission to connect. When a malicious actor sends a large number of SYN packets all at once, the server’s cache is overwhelmed by the traffic generated and stops responding. The connection timeout error message occurs. The logs indicate that a single person spoofed an IP address from an employee and generated a large amount of SYN packets just to try and make the server stop responding to anybody and potentially damage the company. Based on this observation, the conclusion is that the web server was attacked by a DoS SYN flood type of attack.