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: Malicious actors used DoS attack to overwhelm the network with packages making the server shutdown. Maybe Sent from a employees computer. It's not a DDoS attack since there's only one IP address attacking the network. The logs show that: The malicious actors sent many SYN requests in a short amount of time causing the overload in the server. This event could be:Since the requests were from TCP SYN requests and they were coming from an unfamiliar address we can conclude that this is done by the malicious actor, and since it's using unusual number of SYN requests its 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. The [SYN] packet is the initial request from an employee visitor trying to connect to a web page hosted on the web server. SYN stands for "synchronzie." 2. The [SYN,ACK] packet is the web server's response to the visitor's request agreeing to the connection. The server will reserve system resources fro the final step of the handshake. SYN, ACK, stands for "synchronize acknowledge." 3. The [ACK] packet is the visitor's machine acknowledging the permission to connect. This is final step required to make a successful TCP connection. ACK stands for "acknowledge." Explain what happens when a malicious actor sends a large number of SYN packets all at once: It will overwhelm the system from all the SYN requests causing the server to overload and become slow, taking a great amount of time to respond. Explain what the logs indicate and how that affects the server: They indicate that the server is overwhelmed by SYN packet requests and it can't complete the handshake. It affects the server because it overwhelms the server's available resources to reserve for the connection causing the employees not being able to connect.