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 this being a DoS attack on the server. The logs show that there is an abnormal amount of SYN requests. This event could be the work of a malicious actor trying to slow down the server using SYN flooding.

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. A packet is sent to a specific destination with a firewall approving of not approving that connection 2. The connection is accepted or denied 3. The permission is then archived Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor sends a large number of SYN packets all at once this can slow down the server thus causing the port to be shut down. This leads to a denial of service as authentic requests cannot be made as the server is down Explain what the logs indicate and how that affects the server: The logs report an abundance of SYN requests and this leads to the server going down meaning no one can use it, even legit customers