Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
There was an overwhelming amount of SYN requests from the same IP address. This could be a sign of a Denial of Service (DoS) attack due to the large amount of network traffic coming from a single IP address. This can be seen from log 125 to log 152.

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 first step in the handshake is for the [SYN] packet to be sent from the employee trying to connect to the web page on the web server. In this instance [SYN] stands for “synchronize”. 2. The next step in the handshake is the [SYN, ACK] packet which is the web server’s response to the visitor’s initial request, agreeing to the connection. [SYN, ACK] stands for “synchronize acknowledge”. 3. The final step in the handshake is for the [ACK] packet to be sent, which is the visitor's machine acknowledging the permission to connect. Once this last step happens there is a successful TCP connection. When a malicious actor sends a large number of SYN packets all at once, there is a SYN flood. This type of attack targets the network bandwidth to slow traffic. As stated before, the logs indicate that there is a large number of SYN packet requests that are being sent out by a single IP address. This is causing a SYN flood which is making the web server unable to handle the requests.
The next steps that should be taken to fix this problem is to attempt to block the traffic from the threat actor. This can be done by configuring a firewall like a Web Application Firewall or (WAF).