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: The logs show that: There is a large number of TCP SYN requests coming from an unfamiliar IP address This event could be: Direct DNS 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. SYN - The visitor wants to establish a connection with the website. Therefore, a SYN packet is sent which indicates that the visitor is trying to communicate with the server 2. SYN/ACK - Server responds with this packet 3. ACK - The client acknowledges the response from the server Explain what happens when a malicious actor sends a large number of SYN packets all at once: If there is a large number of SYN packets sent to the server, it will have a hard time responding to all of them and thus may leave some requests. This can lead to downtime errors on some visitor's pages. They can refresh the page and send a request again. Explain what the logs indicate and how that affects the server: The log indicates a large number of SYN requests coming from an IP address. This makes it hard for the server to respond to all the requests and thus may lose legitimate traffic.