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 the web server stopped responding to their clients since it is flooded with SYN packets. This event could be classic sign of direct DoS 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 client sends a SYN packet to the web server asking for establishing a new connection. 2. Then, the SYN is acknowledged and in return a SYN, ACK packet is sent back to the client stating that the SYN is received and acknowledged for the new connection. 3. After receiving this SYN, ACK packet, the client sends back a ACK packet back to the web server and hence the connection is established between a website visitor (client) and a web server. Explain what happens when a malicious actor sends a large number of SYN packets all at once. Once the attacker sends a large number of SYN packets all at once, the web server will first try to respond back to it as much as it can based on its potential but later it stops responding to all the SYN packets which resquesting connection to the web server and also stops responding to any other connection and requests. Explain what the logs indicate and how that affects the server: The log indicates that it is a direct DoS attack and server is affecfted by it. Hence, the web server couldn’t respond to anyother connection including the legitimate connection.