Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
The hosting web server could be the target of Denial of Service (Dos) attack. The logs of the time of the incident show that the server was flooded with a wave of TCP SYN packets that it could not keep up with in responding to. Based on these findings, it is likely that the server faced a SYN Flood attack.

Section 2: Explain how the attack is causing the website to malfunction
When a user wants to visit a website, there is a metaphorical handshake that must take place first between the user device and the webserver. This is the TCP Handshake and it is split into three parts. In the first part, the user sends a SYN packet to the server (this is the user device telling the webserver they want to establish a connection with it). Next, the server responds to the user device with a SYN/ACK packet (the server telling the user device that it got its message and will establish a connection with the user). The last part is the user device sending one last ACK packet back to the server (the user device acknowledges that it has been allowed to connect with the server). The attack that our web server was a target consisted of the attacker spam flooding the server with the SYN packet in the first step of the handshake. When the server receives all of these requests to connect, it starts to get overloaded and will eventually stop responding to any requests. The logs of the attack indicate that our hosting server was indeed overloaded by a series of SYN requests, and as a result was not able to form any connections with any new good faith visitors.