Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

There is a large amount of SYN requests from a single IP address that overwhelmed the server, causing it to crash and ignore legitimate user traffic. Since there was a large amount of malicious packets, this attack was a SYN Dos Attack. It was not distributed since there was only one attacker IP address.

Section 2: Explain how the attack is causing the website to malfunction

In order to authenticate a user, the web server receives a SYN packet from the device. The web server then sends a SYN, ACK packet back to the device, which then finally responds with an ACK packet. This process is known as the TCP three-way handshake, and is required to authenticate devices that connect to the web server. The attacker sent a large amount of these SYN requests to the server, and it was unable to handle all of the malicious requests. Thus, the server timed out and was then unable to handle legitimate user traffic. The server could not send SYN/ACK packets out to other users, and the gateway to receive the ACK packets was closing since the server and device were taking too long to communicate.