Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
On September 8th, 2023 at 10:07 AM an automated alert was sent out from the monitoring system highlighting a problem with the web server. Upon a visit to the site, a connection timeout error message is displayed. Upon capturing and analyzing the packets to and from the web server, a large amount of TCP SYN handshake requests are flooding the server from an unfamiliar IP address. This evidence may point towards a potential Dos(Denial of Service) attack, known as a **SYN flood** This attack is currently stopping any legitimate users from accessing the web server, greatly reducing the *availability* of the system

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 host attempting to access the web server will start by sending out a TCP SYN packet 2. The server receives this packet, assigns a response port, then replies with a TCP SYN/ACK packet, returning to the host IP address 3.Once the host receives this packet, a ACK packet is sent back to the server, establishing the TCP handshake and allowing data transfer Explain what happens when a malicious actor sends a large number of SYN packets all at once:This form of an attack overwhelms the server, consuming all of its resources and using up all the ports, severely reducing the overall efficiency of the system and most of the time, completely disabling the system for a long period of time without IT interference. The reduced availability of the site has a great impact on the overall function and reputation of the company since customers and legitimate users have no way of accessing what they need. This can be remedied by updating the firewall to block the malicious IP address from sending requests to the server, however the attacker can change their IP address. It is recommended that we pursue more preventative measures in the future like: -Load balancing(distributing traffic through multiple networks) -Rate Limiting(Limit the rate at which traffic reaches the server)