SYN Flood: Cybersecurity Incident Report

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

The company's website became inaccessible due to a denial-of-service (DoS) attack that overwhelmed the web server with traffic. The attack was detected through automated monitoring that sent an alert about the unresponsive web server.

Analysis of TCP/HTTP network traffic in Wireshark revealed a flood of TCP SYN requests sent to the web server from a single unfamiliar IP address. At first, the server managed to respond to the requests while still handling some legitimate traffic. However, the volume of SYN requests eventually exceeded the server's capacity, using up all available ports.

With all its resources tied up responding to attack requests, the server could no longer handle any legitimate user traffic. This resulted in visitors receiving connection timeout errors when attempting to access the website. The attack is characterized as a SYN flood denial-of-service attack rather than a distributed denial-of-service (DDoS) attack since the malicious traffic originated from just one IP address rather than a botnet of devices.

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

A SYN flood attack is when a malicious actor abuses the TCP handshake process and repeatedly sends requests to connect to the web server. The server tries to respond to each one of these requests but only has so many ports available to do so, and the attacker’s goal is to send more requests than the amount of server ports.

At first, the attack will slow the network down and users may experience long loading times when visiting the site but eventually the server will become too overwhelmed and will be completely unable to operate.

The consequences of this attack include loss of revenue due to inability to complete regular business operations, loss of customer trust, and potential damages to the server and its data.

There are many ways to prevent future attacks like this such as:

- Using a Next Generation Firewall (NGFW) to proactively monitor the network for suspicious activity
- Using VPNs and encryption to conceal the IP address of the web server
- Using subnets to ensure that one outage does not affect/spread to the entire organization’s infrastructure.