SYN Attack Incident Report

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

This attack was identified after our monitoring system triggered an automated alert indicating an issue with the web server. Currently, attempting to access the company's website results in a connection timeout error.

Upon analyzing the network traffic with Wireshark, a protocol analyzer, the cybersecurity team observed an unusually high volume of TCP SYN requests originating from an unfamiliar IP address. Initially, the server was able to respond to these requests and maintain normal operations, but the overwhelming number of SYN requests eventually caused the server to become overloaded, preventing it from responding to legitimate traffic.

This attack appears to be a Denial of Service (DoS) SYN flood attack. The flood of SYN requests is coming from a single IP address, meaning the attacker is not currently using multiple devices to launch a Distributed Denial of Service (DDoS) attack. However, the sheer volume of SYN requests has exceeded the web server's capacity, causing it to become unresponsive and resulting in connection timeout errors for users attempting to access the site.

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

A SYN flood attack occurs when a malicious actor exploits the TCP handshake process by continuously sending connection requests to the web server. The server attempts to respond to each request, but it has a limited number of ports available for connections. The attacker's objective is to overwhelm the server by sending more requests than it can handle.

Initially, the attack may slow down the network, causing users to experience longer loading times when trying to access the site. However, as the attack progresses, the server will become overwhelmed to the point where it can no longer function properly.

The impact of this attack includes financial losses due to the inability to carry out regular business activities, erosion of customer trust, and potential damage to the server and its data.