SYN Flood: Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
The attack was identified following an automated alert from our monitoring system, which flagged an issue with the web server. When attempting to access the company's website, users are met with a connection timeout error message. Upon analyzing the situation with Wireshark, a network protocol analyzer, the cybersecurity analyst found an unusually high number of TCP SYN requests originating from an unfamiliar IP address. Initially, the server could respond to these requests and maintain regular operations, but the sheer volume eventually overwhelmed it, preventing it from handling legitimate requests. This attack appears to be a Denial of Service (DoS) SYN flood attack. The influx of SYN requests is coming from a single IP address, indicating that the attacker is not employing multiple devices to create a Distributed Denial of Service (DDoS) attack. The excessive SYN requests exceed the number of ports the web server can handle, causing it to become unresponsive and resulting in connection timeout errors for anyone trying to visit 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 repeatedly sending connection requests to a web server. The server attempts to respond to each request but has a limited number of ports available. The attacker’s goal is to exceed the number of available server ports with their requests. Initially, the attack will slow down the network, causing users to experience long loading times when visiting the site. Eventually, the server becomes overwhelmed and unable to operate altogether. The consequences of this attack include loss of revenue due to disrupted business operations, loss of customer trust, and potential damage to the server and its data. To prevent future attacks like this, consider the following measures: ● Implement a Next Generation Firewall (NGFW) to proactively monitor the network for suspicious activity. ● Use VPNs and encryption to conceal the web server's IP address. ● Employ subnets to ensure that an outage in one area does not affect the entire organization’s infrastructure.