Cybersecurity Incident Report

Scenario

Review the following scenario. Then complete the step-by-step instructions.

You work as a security analyst for a travel agency that advertises sales and promotions on the company's website. The employees of the company regularly access the company's sales webpage to search for vacation packages their customers might like.

One afternoon, you receive an automated alert from your monitoring system indicating a problem with the web server. You attempt to visit the company's website, but you receive a connection timeout error message in your browser.

You use a packet sniffer to capture data packets in transit to and from the web server. You notice a large number of TCP SYN requests coming from an unfamiliar IP address. The web server appears to be overwhelmed by the volume of incoming traffic and is losing its ability to respond to the abnormally large number of SYN requests. You suspect the server is under attack by a malicious actor.

You take the server offline temporarily so that the machine can recover and return to a normal operating status. You also configure the company's firewall to block the IP address that was sending the abnormal number of SYN requests. You know that your IP blocking solution won't last long, as an attacker can spoof other IP addresses to get around this block. You need to alert your manager about this problem quickly and discuss the next steps to stop this attacker and prevent this problem from happening again. You will need to be prepared to tell your boss about the type of attack you discovered and how it was affecting the web server and employees.

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

According to the Wireshark TCP/HTTP log, there were many SYN request coming from an unfamiliar IP address but the requests coming from one IP address. This overwhelms server resources and preventing it from establishing a connection. So, the attack is likely a Denial of Service (DoS) or TCP SYN flood attack.

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

The SYN Flood attack is causing the website to malfunction by exploiting the way TCP connections are established. In a normal TCP handshake, the client sends a SYN (synchronize) request to the server, the server responds with a SYN-ACK (synchronize-acknowledge) packet, and finally, the client sends an ACK (acknowledge) packet to establish the connection. However, in a SYN Flood attack, the attacker sends a massive number of SYN requests to the target server but doesn't respond to the server's SYN-ACK packets. This leads to the server keeping many pending half-open connections, tying up its resources and preventing it from processing legitimate connection requests. As a result, the web server becomes overwhelmed and unable to handle incoming user requests, leading to connection timeouts and a denial of service for legitimate users.

The attack's impact is twofold: First, the sheer volume of pending half-open connections exhausts the server's available resources, such as memory and processing power. This impairs the server's ability to process incoming requests, including those from employees accessing the sales webpage. Second, the server's inability to establish new connections due to the flood of SYN requests results in connection timeouts for legitimate users, rendering the website inaccessible. By exploiting the TCP handshake process, the attacker effectively paralyzes the web server's ability to serve its intended users, causing disruption and rendering the website unusable for its intended purpose of advertising sales and promotions.