Cybersecurity Incident 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.

Cybersecurity Incident Report

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

An automated alert indicated a problem with the company’s web server. Using a packet sniffer, the security team identified an abnormally large number of TCP SYN requests originating from an unfamiliar IP address. This behavior is consistent with a SYN flood attack, which is a form of Denial-of-Service (DoS) attack designed to overwhelm a server and disrupt normal operations.

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

A SYN flood attack exploits the TCP 3-way handshake. Normally, a client initiates a connection by sending a SYN packet, the server responds with a SYN-ACK, and the client finalizes the connection with an ACK. In this attack, the malicious actor sends a flood of SYN requests but does not complete the handshake. This causes the server to allocate resources for numerous half-open connections. As the volume of these incomplete connections increases, the server’s resources are exhausted, preventing it from responding to legitimate requests. This results in connection timeout errors for users attempting to access the website.