Security Incident Report

Analyzing Network Attacks

Wendy Alayon
09/06/2024 **@syszern**

Table of Contents

Security incident report

Scenario

A security analyst at a travel agency, responsible for advertising sales and promotions on the company's website, received an automated alert from the monitoring system indicating an issue with the web server. Employees regularly accessed the company's sales webpage to search for vacation packages for their customers.

One afternoon, the security analyst attempted to visit the company's website but encountered a connection timeout error message in the browser.

To diagnose the issue, the analyst utilized a packet sniffer to capture data packets in transit to and from the web server. Upon analysis, a large number of TCP SYN requests were observed originating from an unfamiliar IP address. The web server appeared to be overwhelmed by the volume of incoming traffic, leading to a degradation in its ability to respond to the abnormally large number of SYN requests. This indicated a potential attack by a malicious actor.

In response, the security analyst temporarily took the server offline to allow it to recover and return to normal operating status. The analyst then configured the company's firewall to block the IP address responsible for the abnormal traffic. However, recognizing that this IP blocking solution was a temporary measure, as an attacker could spoof other IP addresses to bypass the block, the analyst prepared to alert the manager about the issue and discuss the next steps.

The analyst needed to be prepared to explain to the manager the type of attack discovered, its impact on the web server and employees, and propose preventive measures to stop the attacker and prevent future incidents.

Determining the Type of Attack Behind the Network Interruption

The website's connection timeout error message may be attributed to an excessive influx of TCP SYN requests originating from an unfamiliar IP address. This surge overwhelms the server, rendering it unable to manage the incoming requests from legitimate users effectively. As evidenced by the logs, the server struggles to keep up with the unusually high volume of SYN requests pouring in rapidly. The attacker is persistently sending multiple SYN requests every second, causing disruptions highlighted by yellow-labeled failed communications between genuine website visitors and the server. Notably, analysis of the logs reveals that all requests originate from the same IP address, suggesting a coordinated attack. This pattern strongly suggests a SYN flood attack, a type of Denial of Service (DoS) attack wherein the server is bombarded with an abnormal number of SYN requests during the TCP handshake process. Consequently, the server becomes incapacitated, unable to respond to requests and leading to a disruption in service.

Describing How the Attack Is Disrupting Website Operations

When website visitors attempt to connect with the web server, a three-way handshake takes place using the TCP protocol. The handshake involves three distinct steps:

1. The [SYN] packet represents the initial connection request made by a visitor, who is an employee, aiming to access a web page hosted on the web server. SYN signifies "synchronize."

2. The [SYN, ACK] packet serves as the web server's response to the visitor's request, signaling agreement to establish the connection. In this phase, the server allocates system resources in anticipation of completing the handshake process. SYN, ACK denotes "synchronize acknowledge".

3. The [ACK] packet signifies acknowledgment from the visitor's machine, confirming permission to establish the connection. This final step is crucial for completing a successful TCP connection. ACK represents "acknowledge."

However, malicious actors can exploit the TCP protocol through a tactic known as a SYN flood attack. This technique involves flooding the server with an overwhelming volume of SYN packet requests, overwhelming its resources. As a result, the server finds it challenging to manage the influx of SYN packets, hampering its capacity to handle genuine traffic. This leads to the server becoming unresponsive to legitimate requests, causing disruptions in service for genuine users.

The symptoms of a SYN flood attack typically include rapid influx of SYN packets from a single or multiple sources, increased server resource consumption without successful connections established, and unresponsiveness of the server to legitimate requests.

The logs indicate a SYN flood attack targeting the TCP handshake process. The attack overwhelms the server with SYN packet requests, disrupting the flow of traffic and resulting in connection timeout errors for users attempting to access the website.

The consequences of such an attack can be severe for the organization such as loss of revenue due to downtime and inability to serve customers, damage to the organization's reputation and customer trust, and potential data loss or leakage if the attack compromises sensitive information.

To mitigate the risk of future attacks, the organization can implement utilizing firewalls and intrusion detection/prevention systems to filter and block malicious traffic, implementing rate-limiting measures to restrict the number of incoming SYN requests from individual IP addresses, regularly updating and patching network infrastructure and server software to address known vulnerabilities.