Justin Goncalves

7/21/24

Cybersecurity Network Attack Analysis Project

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.

How to read the Wireshark TCP/HTTP Logs: How to read a Wireshark TCP/HTTP log

Follow the instructions and answer the question to complete the activity.

Section 1: Identify the type of attack that may have caused this network interruption
Network attacks are malicious attempts to disrupt, damage, or gain unauthorized access to computer networks. These attacks can vary widely in their methods and impact, including Denial of Service (DoS), Distributed Denial of Service (DDoS), Man-in-the-Middle (MitM), phishing, and ransomware attacks. Each type exploits different vulnerabilities and has distinct signatures and impacts on network performance and security.

The symptoms described in the scenario—specifically, a large number of TCP SYN requests from an unfamiliar IP address overwhelming the web server—are indicative of a SYN flood attack. This type of attack is a subset of Denial of Service (DoS) attacks. In a SYN flood attack, an attacker sends a flood of TCP/SYN packets, often with spoofed IP addresses, to exhaust server resources and prevent legitimate traffic from being processed.

The difference between a Denial of Service (DoS) and a Distributed Denial of Service (DDoS) attack lies in the source of the attack. A DoS attack originates from a single source targeting a specific server or network, aiming to exhaust its resources and make it unavailable to legitimate users. In contrast, a DDoS attack involves multiple sources, often part of a botnet, attacking the target simultaneously. This makes DDoS attacks harder to mitigate because the malicious traffic comes from numerous sources, making it difficult to distinguish between legitimate and illegitimate traffic.

The website is taking a long time to load and reporting a connection timeout error because the web server is overwhelmed by the volume of incoming SYN requests. This overload prevents the server from responding to legitimate connection requests, causing delays and timeouts. The logs captured by the packet sniffer reveal a large number of these SYN requests originating from an unfamiliar IP address, directed at the web server, which is unable to handle the excessive traffic, leading to connection timeouts and making the website inaccessible to legitimate users. This disruption affects the overall availability and performance of the web server, leading to a denial of service.

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

When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. The first step involves the client sending a SYN packet to the server to initiate the connection. In the second step, the server responds with a SYN-ACK packet, acknowledging the client's request and synchronizing the connection. The third step is when the client sends an ACK packet back to the server, completing the handshake and establishing the connection.

The SYN flood attack is characterized by the attacker sending an overwhelming number of TCP SYN packets to the server without completing the handshake process. The server, in response, allocates resources for each incoming SYN packet and sends back SYN-ACK packets. However, since the attacker does not send the final ACK packet to complete the handshake, the server's connection table becomes filled with half-open connections. This prevents the server from processing new legitimate connections, leading to symptoms such as connection timeouts and the server becoming unresponsive to valid traffic. The logs captured by the packet sniffer reveal this pattern, with repeated SYN requests from an unfamiliar IP address overwhelming the server.

This attack significantly affects the organization’s network by consuming server resources and rendering the web server unable to handle legitimate traffic. The website takes a long time to load and often times out, preventing employees and customers from accessing essential services and information. This disruption can lead to lost sales, decreased customer satisfaction, and potential reputational damage. Additionally, prolonged unavailability of the website can impact business operations, especially if the site is a critical point of interaction for customers.

To prevent such attacks in the future, several measures can be implemented. These include deploying SYN cookies, which allow the server to handle SYN requests without allocating resources until the handshake is completed, implementing rate limiting to restrict the number of SYN packets from a single IP address, and using a Web Application Firewall (WAF) to filter and monitor traffic. Additionally, investing in Distributed Denial of Service (DDoS) protection services can help mitigate the impact of large-scale attacks by absorbing and managing malicious traffic before it reaches the web server. Regular security audits and penetration testing can also help identify and address vulnarabilities in the network infrastructure.