Cybersecurity Incident Report

By Jovworie Tanshi

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
One potential explanation for the website's connection timeout error message is: The website may be experiencing a Denial of Service (DoS) attack, specifically a SYN flood attack. This type of attack occurs when a malicious actor sends a large number of TCP SYN requests to a web server. These requests initiate TCP connections but do not complete the handshake, causing the server to allocate resources for these half-open connections and eventually become overwhelmed. **The logs show that:** An unusually high number of TCP SYN requests are being sent to the web server.

These requests are originating from an unfamiliar IP address.
The web server is losing its ability to respond to legitimate traffic due to the volume of SYN requests.

This event could be: A SYN flood attack, which is a type of Denial of Service (DoS) attack. This attack aims to exhaust the resources of the web server by flooding it with SYN packets, causing it to become unresponsive to legitimate traffic and leading to connection timeout errors for users trying to access the website.

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. Explain the three steps of the handshake:

- **SYN (Synchronize):**

The client sends a TCP SYN packet to the server to initiate a new connection.

- **SYN-ACK (Synchronize-Acknowledge):**

The server responds with a TCP SYN-ACK packet, acknowledging the client's request to establish a connection.

- **ACK (Acknowledge):**

The client sends an ACK packet back to the server, completing the three-way handshake and establishing a TCP connection.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor sends a large number of SYN packets all at once, the server receives these connection requests and allocates resources to handle each one, entering the half-open state (waiting for the ACK from the client to complete the handshake). However, because the attacker does not send the final ACK packet to complete the handshake, the server's resources remain tied up, waiting for a response that never comes. This overwhelms the server, exhausting its available resources and preventing it from handling legitimate connection requests, leading to a denial of service for genuine users.

Explain what the logs indicate and how that affects the server: The logs indicate an unusually high volume of incoming TCP SYN requests from an unfamiliar IP address. This abnormal activity suggests a SYN flood attack. The impact on the server is significant:

- **Resource Exhaustion:** The server allocates resources to handle the SYN requests, but these resources remain tied up due to the lack of completion of the handshake.

- **Inability to Serve Legitimate Requests:** As the server becomes overwhelmed with the half-open connections, it loses its ability to respond to legitimate traffic, leading to connection timeout errors for genuine users trying to access the website.

- **Performance Degradation:** The overall performance of the server degrades as it

struggles to manage the flood of SYN requests, further impacting the user experience and potentially leading to a complete denial of service.

In summary, the SYN flood attack exploits the TCP handshake process to overload the server with half-open connections, depleting its resources and rendering it unable to serve legitimate users, which results in connection timeouts and website unavailability.