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

The log shows the occurrence of a SYN flood attack, a type of DoS attack. The attacker's IP address (203.0.113.0) sends many SYN packets through the TCP protocol to the web server. The attacker floods the web server with SYN packets, preventing it from responding to legitimate requests.

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

The attack:

One afternoon, an automated alert indicated a problem with the web server. When a request is made over the TCP protocol, the three-way handshake process is used to establish a connection.

- The initial request is the [SYN] packet. A request to synchronize between the source and destination.
- The response is the [SYN, ACK] packet, agreeing to the connection. The synchronization request is acknowledged and the server reserves resources for the last step of the handshake.
- The last step is the [ACK] packet, acknowledging the permission to connect.

Legitimate website visitors experience connection issues, and one visitor from the log receives a "504 Gateway Time-out" error message, while another receives an [RST, ACK] packet, indicating a dropped connection attempt. After reviewing the logs, it appears there are many TCP SYN requests made by an unknown IP address to the webserver (192.0.2.1). This meets the criteria of a SYN flood attack, a type of DoS attack.

The affect:

By continuously requesting connection to the webserver using the TCP SYN flood attack, the website malfunctions as the server's resources are being overwhelmed. The webserver attempts to respond to all requests and isn't aware that it is being attacked. This prevents it from responding to legitimate requests and disrupting the normal communication between website visitors and the server, resulting in a denial of service.

The consequences:

This negative result prevents sales and promotions from occurring, hindering revenue for the time the service remains unavailable. This downtime and disrupted operations can also have a negative effect on reputation and internal resources. Depending on the downtime and products/services sold, this can have a detrimental affect on the organization's reputation. Regarding the internal resources, IT and incident response personnel will need to be made available which could leave other sections of the security posture unmanned during the time it takes to resolve the issue.

The remediation:

One potential way to secure the network and prevent future attacks would be to implement a Next Generation Firewall (NGFW). In doing so, it may be able to detect the pattern of a DoS attack and block the IP addresses that it uses. Another way would be to deploy Load Balancers, doing this would alleviate the load and distribute it evenly among other web servers to allow for the connections to be made to the requests. Lastly, it is recommended to develop and revise the Incident Response Planning relating to a DoS attack, specifically the SYN flood attack. As there is always a way for an attacker to disrupt any organization's operations, it is advised to be prepared in any event.