Project: Analyze Network Attacks

Cybersecurity Incident Report

Scenario

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 logs show that: There are flood of SYN packets coming from the same IP Address.

This event could be: This could be a DoS attack as they are using SYN packets to flood the network to cause network interruption to a specific server.

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:
1. Send a SYN request is sent from the source to destination.

2. Destination responds with SYN/ACK to acknowledge receipt of request for source and leaves port open

3. An ACK packet is sent from source to destination. Then TCP connection is established.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: The server becomes overwhelmed the servers available resources to reserve for connection. This can cause the server to not function causing it either to crash or timeout.

Explain what the logs indicate and how that affects the server: The logs indicate that there is a SYN flood attack on the server, not allowing visitor's to connect. Visitor's are getting timeout messages because there aren't enough ports due to the amount of syn packets overwhelming the server.