Case Study:

Analyze Network Attacks - Incident Reporting

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.

Incident Report

Theory on Type of Attack:

My theory is that this event could be a type of Denial of Service (DoS) attack, specifically SYN flooding. It would not only provide an explanation for the website's connection timeout error but also explain the results of the logs from the packet sniffer showing that the web server stops responding after it is overloaded with SYN packet requests.

In-Depth Explanation

In order for customers or users to visit the website, per the TCP protocol, a three-way handshake must occur to establish a connection with the web server. If everything executes according to plan, it looks like this:

- A SYN packet is sent from the source to the destination, requesting to connect.
- The destination replies with a SYN-ACK packet to accept the connection request and reserve resources for the source to connect.
- Then a final ACK packet is sent from the source to the destination which acknowledges the permission to connect.

However, during this SYN flood attack, a malicious actor is sending a large number of SYN packets all at once. As a result, the server's available resources are overwhelmed and a legitimate TCP connection cannot be established.

The logs from the packet sniffer confirm that the web server has become overwhelmed and is unable to process new SYN requests which is why visitors are receiving a connection timeout message during this DoS attack.