Incident Report

3rd February 2025

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

Jefferson Yankson

about the type of attack you discovered and how it was affecting the web server and employees.

Cybersecurity Incident Report

Section 1: The type of attack that may have caused this network interruption
One potential explanation for the website's connection timeout error message is a DoS attack. The logs show that the web server has received an increasing amount of traffic from an unknown IP address. This event could be a SYN flood attack, a type of DoS attack that stimulates a TCP connection and floods a server with SYN packets

Section 2: 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 source device sends a synchronize (SYN) request to a server, requesting a connection. The server responds with a SYN-ACK packet, acknowledging the request. Once the server receives the final ACK packet from the source and acknowledges the request, a TCP connection is established. In the case of a SYN flood attack, from the log, the web server receives an immense amount of SYN requests, overwhelming the server's processing capabilities to accept new requests from clients.

Jefferson Yankson