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

Cybersecurity Incident Report

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: SYN flood attack The logs show that: A large number of TCP SYN requests from an unknown IP This event could be: Ip spoofing and/or SYN Flood Attack

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 connection. **SYN-ACK (Synchronize-Acknowledge):** The server responds with a SYN-ACK packet, acknowledging the client's SYN request and indicating readiness to establish a connection. **ACK (Acknowledge):** The client sends an ACK packet back to the server, completing the connection setup and allowing data transfer to begin. Explain what happens when a malicious actor sends a large number of SYN packets all at once: The server tries to process each SYN request and waits for the corresponding ACK packets from the client. The server may become overwhelmed by these requests and prevent new connections from happening. Explain what the logs indicate and how that affects the server: The logs indicate a large number of incoming TCP SYN requests from an unfamiliar IP address. This abnormal surge in SYN requests overwhelms the server, filling its connection table with half-open connections and causing it to lose its ability to respond to new connection attempts. As a result, the server becomes unresponsive, leading to connection timeout errors for legitimate users, and interrupting the company's operations.