Cybersecurity Incident Report

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

Users are seeing a "connection timeout error." I've checked the logs, and it appears our system was overwhelmed by a high volume of TCP requests, all originating from the IP address `203.0.113.0`. This activity strongly indicates a Denial of Service (DoS) attack, likely from a malicious actor using that IP. Bringing this to your attention immediately.

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.

1. The **client** initiates the connection by sending a TCP segment with the **SYN (Synchronize Sequence Numbers)** flag set to the server. The client then enters the `SYN-SENT` state, waiting for a response.

2. If the server is willing to establish the connection, it responds with a TCP segment that has both the **SYN** and **ACK (Acknowledgment)** flags set. The server then enters the `SYN-RECEIVED` state.

3. Finally, the **client** receives the server's SYN-ACK packet. It sends back a TCP segment with the **ACK** flag set. Upon sending this ACK, the client enters the `ESTABLISHED` state. When the server receives this final ACK, it also moves to the `ESTABLISHED` state. At this point, the TCP connection is fully established, and data transfer can begin.

Because the source IP addresses in the malicious SYN packets are spoofed or belong to hosts not actually initiating the connection, the server will **never receive the final ACK** packet (Step 3 of the handshake) for these requests. The attacker sends SYN packets at a rate faster than the server can clear out the timed-out half-open connections. This causes the server's SYN queue (the backlog of pending connections) to fill up. Once the SYN queue is full, the server can no longer accept new, legitimate connection requests from actual users.