Cybersecurity Incident Report:

Security Issue When Accessing Company Website

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 that our web server is overloaded with SYN requests and is unable to fulfill them hence why customers are not able to establish a successful handshake. The logs show that there is an initial successful handshake via the Transmission Control Protocol from an unfamiliar IP address 203.0.113.0. Shortly after, there are several SYN

packet requests received by our web server from the same IP address.

This event could be a direct DoS SYN flood attack on our web 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. Source IP will send a SYN (Synchronise) packet request to the destination IP to accept.

2. Destination IP will acknowledge the SYN packet from the source IP and will send a SYN/ACK (Synchronise & Acknowledge) packet back to the source IP. The destination will reserve resources for the source to connect.

3.Source IP receives SYN/ACK packet and will send back the ACK packet to complete the handshake via TCP.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:
When a malicious actor sends a large number of SYN packets all at once to a destination, the destination web server in this case will become overloaded and unable to fulfill other SYN packet requests as all of the reserved resources have been used up. Instead, users will get back a RST(Reset)/ACK packet which is causing the timeout error to occur as the connection was dropped.

Explain what the logs indicate and how that affects the server:
The logs indicate several SYN packet requests from the abnormal IP address 203.0.113.0, transmitted to our web server. The web server becomes too overloaded from these SYN packet requests therefore it cannot keep up with fulfilling these requests. This causes the web server to stop responding entirely to all SYN packet requests.