SYN Flood: 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** |
| This attack was discovered after an automated alert from our monitoring system indicated a problem with the web server. After attempting to visit the company’s website, you will only receive a connection timeout error message.  When using Wireshark TCP/HTTP log, a network protocol analyzer, the cybersecurity analyst discovered that there were a very large number of TCP SYN requests coming from an unfamiliar IP address. The server was initially able to respond to them and continue with regular operations, but the volume was so much that the server became overwhelmed and unable to respond to legitimate requests.  This attack is likely a Denial of Service (DoS) SYN flood attack. The large amount of SYN requests came from only one IP address so the attacker currently is not using more than one device to create a Distributed Denial of Service (DDoS) attack. Due to the amount of SYN requests eventually becoming greater than the number of ports that the web server can handle, the server is no longer able to fill requests and any attempt to visit the site will result in a connection timeout error. |
|  |

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| A SYN flood attack is when a malicious actor abuses the TCP handshake process and repeatedly sends requests to connect to the web server. The server tries to respond to each one of these requests but only has so many ports available to do so, and the attacker’s goal is to send more requests than the amount of server ports.  At first, the attack will slow the network down and users may experience long loading times when visiting the site but eventually the server will become too overwhelmed and will be completely unable to operate.  The consequences of this attack include loss of revenue due to inability to complete regular business operations, loss of customer trust, and potential damages to the server and its data.  There are many ways to prevent future attacks like this such as:   1. Using a Next Generation Firewall (NGFW) to proactively monitor the network for suspicious activity 2. Using VPNs and encryption to conceal the IP address of the web server 3. Using subnets to ensure that one outage does not affect/spread to the entire organization’s infrastructure. |