Activity Overview

In this activity, you will consider a scenario involving a customer of the company that you work for who experiences a security issue when accessing the company's website. You will identify the likely cause of the service interruption. Then, you will explain how the attack occurred and the negative impact it had on the website.

In this course, you have learned about several common network attacks. You have learned their names, how they are carried out, and the characteristics of each attack from the perspective of the target. Understanding how attacks impact a network will help you troubleshoot issues on your organization's network. It will also help you take steps to mitigate damage and protect a network from future attacks. To review attacks, visit Identify: Network Attacks

Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

Scenario

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.

Reflect on the types of network intrusion attacks that you have learned about in this course so far. As a security analyst, identifying the type of network attack based on the incident is the first step to managing the attack and preventing similar attacks in the future.

Here are some questions to consider when determining what type of attack occurred:

- What do you currently understand about network attacks?
- Which type of attack would likely result in the symptoms described in the scenario?
- What is the difference between a denial of service (DoS) and distributed denial of service (DDoS)?
- Why is the website taking a long time to load and reporting a connection timeout error?

Review the Wireshark reading from step 2 and try to identify patterns in the logged network traffic. Analyze the patterns to determine which type of network attack occurred. Write your analysis in section one of the Cybersecurity incident report template provided.

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: is that a threat actor is using a syn flood attack that is overwhelming the server. This will exhaust the web server's resources making it incapable of responding appropriately to legitimate traffic The logs show that: The web server stops responding after it is overloaded with SYN packet requests. This event could be: A DOS or denial of service 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: 1. A SYN packet is sent from the source to the destination, requesting to connect. 2. The destination replies to the source with a SYN-ACK packet to accept the connection request. The destination will reserve resources for the source to connect. 3. A final ACK packet is sent from the source to the destination acknowledging the permission to connect. Explain what happens when a malicious actor sends a large number of SYN packets all at once: In the case of a SYN flood attack, a malicious actor will send a large number of SYN packets all at once, which overwhelms the server's available resources to reserve for the connection. When this happens, there are no server resources left for legitimate TCP connection requests. Explain what the logs indicate and how that affects the server: The logs indicate that the web server has become overwhelmed and is unable to process the visitors' SYN requests. The server is unable to open a new connection to new visitors who receive a connection timeout message.