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.

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.

Instructions:

1. Identify the type of attack causing this network interruption

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.

2. Explain how the attack is causing the website to malfunction

Review the Wireshark reading from step 2, then write your analysis in section two of the Cybersecurity incident report template provided.

When writing your report, discuss the network devices and activities that are involved in the interruption. Include the following information in your explanation:

- Describe the attack. What are the main symptoms or characteristics of this specific type of attack?
- Explain how it affected the organization's network. How does this specific network attack affect the website and how it functions?
- Describe the potential consequences of this attack and how it negatively affects the organization.
- *Optional:* Suggest potential ways to secure the network so this attack can be prevented in the future.