Portfolio Project

Analysing Network Layer Communication

Google Cybersecurity Professional Certificate

Prepared by :
Aleck Kitenge

1 Activity Overview

In this activity, you will analyse DNS and ICMP traffic in transit using data from a network protocol analyser tool. You will identify which network protocol was utilised in assessment of the cybersecurity incident.

In the internet layer of the TCP/IP model, the IP formats data packets into IP datagrams. The information provided in the datagram of an IP packet can provide security analysts with insight into suspicious data packets in transit.

Knowing how to identify potentially malicious traffic on a network can help cybersecurity analysts assess security risks on a network and reinforce network security.

Review the scenario below. Then complete the step-by-step instructions.

You are a cybersecurity analyst working at a company that specializes in providing IT consultant services. Several customers contacted your company to report that they were not able to access the company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.

You are tasked with analysing the situation and determining which network protocol was affected during this incident. To start, you visit the website and you also receive the error “destination port unreachable.” Next, you load your network analyser tool, tcpdump, and load the webpage again. This time, you receive a lot of packets in your network analyser. The analyser shows that when you send UDP packets and receive an ICMP response returned to your host, the results contain an error message: “udp port 53 unreachable.”

2

Activity Logs

```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```

3 Activity Questions

Provide a summary of the problem found in the DNS and ICMP traffic log

The network traffic analyzer tool inspects all IP packets traveling through the network interfaces of the machine it runs on. Network packets are recorded into a file. After analyzing the data presented to you from the DNS and ICMP traffic log, identify trends in the data. Assess which protocol is producing the error message when resolving the URL with the DNS server for the yummyrecipesforme.com website. Recall that one of the ports that is displayed repeatedly is port 53, commonly used for DNS.

In your analysis:

·Include a brief summary of the DNS and ICMP log analysis and identify which protocol was used for the ICMP traffic.

·Provide a few details about what was indicated in the logs.

·Interpret the issues found in the logs.

Record your responses in part one of the cybersecurity incident report.

Explain your analysis of the data and provide one solution to implement

Now that you've inspected the traffic log and identified trends in the traffic, describe why the error messages appeared on the log. Use your answer in the previous step and the scenario to identify the reason behind the ICMP error messages. The error messages indicate that there is an issue with a specific port. What do the different protocols involved in the log reveal about the incident?

In your response:

·State when the problem was first reported.

·Provide the scenario, events, and symptoms identified when the event was first reported.

·Describe the information discovered while investigating the issue up to this point.

·Explain the current status of the issue.

·Provide the suspected root cause of the problem.

Record your responses in part two of the cybersecurity incident report.

4 Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log

The network analysis results show that the DNS server is down or unreachable. This is because the ICMP echo reply returned the error message "udp port 53 unreachable." Port 53 is commonly used for DNS traffic, so this error message indicates that the DNS server is likely not responding.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

At 1:23 PM today, customers began reporting that they were receiving a "destination port unreachable" error message when trying to visit the website. The organization's network security team is investigating the issue so that customers can access the website again.

Using tcpdump, we conducted packet sniffing tests and found that DNS port 53 was unreachable. The next step is to determine whether the DNS server is down or if traffic to port 53 is being blocked by the firewall. The DNS server may be down due to a successful denial-of-service attack or a misconfiguration.