Analyzing Network Using (tcpdump)

Introduction

This presentation covers three key aspects of the project: the scenario, the notes used, and the final result. The scenario outlines the project goals, the notes provide guidance, and the final project demonstrates how these elements were applied.

Scenario:

Activity Overview

In this activity, you will analyze DNS and ICMP traffic in transit using data from a network protocol analyzer tool. You will identify which network protocol was utilized 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.

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 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 analyzing 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 analyzer tool, tcpdump, and load the webpage again. This time, you receive a lot of packets in your network analyzer. The analyzer 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.”

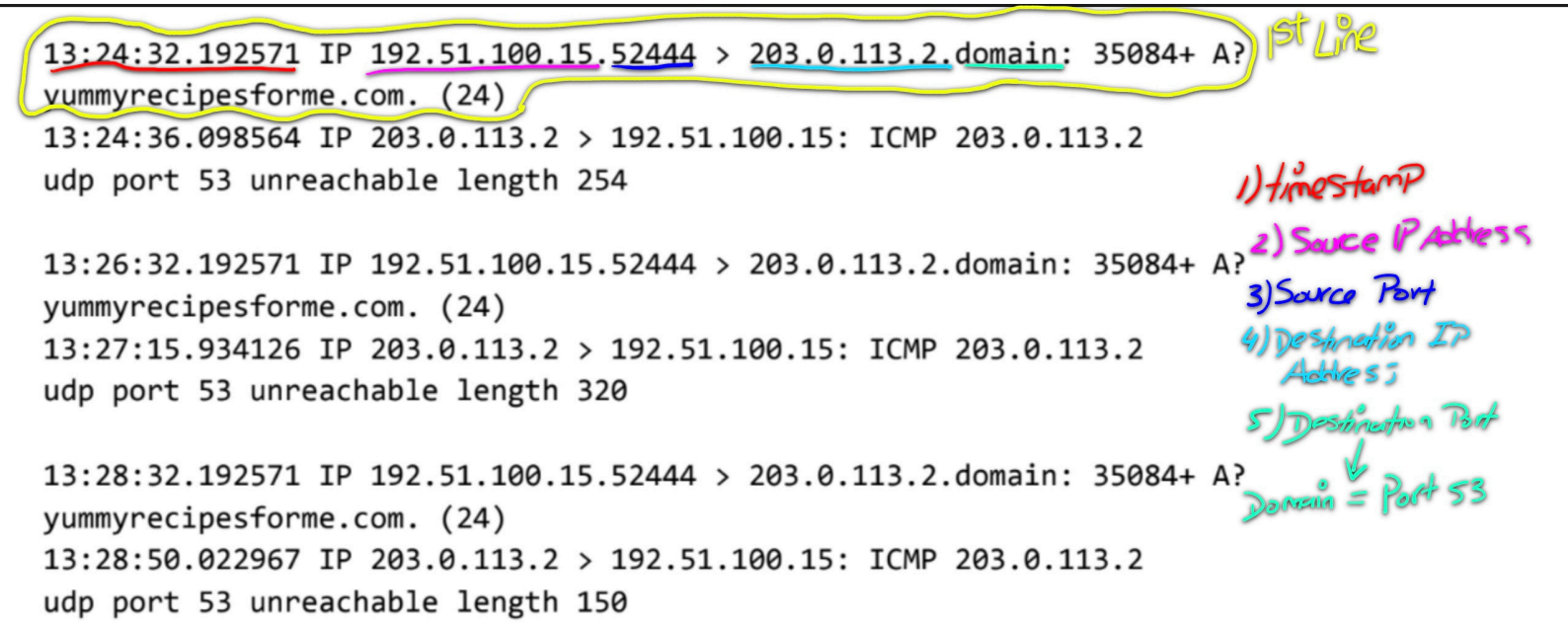
Notes:

In the DNS and ICMP log, you find the following information:

1. In the first two lines of the log file, you see the initial outgoing request from your computer to the DNS server requesting the IP address of yummyrecipesforme.com. This request is sent in a UDP packet.
2. Next you find timestamps that indicate when the event happened. In the log, this is the first sequence of numbers displayed. For example: 13:24:32.192571. This displays the time 1:24 p.m., 32.192571 seconds.
3. The source and destination IP address is next. In the error log, this information is displayed as: 192.51.100.15.52444 > 203.0.113.2.domain. The IP address to the left of the greater than (>) symbol is the source address. In this example, the source is your computer's IP address. The IP address to the right of the greater than (>) symbol is the destination IP address. In this case, it is the IP address for the DNS server: 203.0.113.2.domain
4. The second and third lines of the log show the response to your initial ICMP request packet. In this case, the ICMP 203.0.113.2 line is the start of the error message indicating that the ICMP packet was undeliverable to the port of the DNS server.
5. Next are the protocol and port number, which displays which protocol was used to handle communications and which port it was delivered to. In the error log, this appears as: udp port 53 unreachable. This means that the UDP protocol was used to request a domain name resolution using the address of the DNS server over port 53. Port 53, which aligns to the .domain extension in 203.0.113.2.domain, is a well-known port for DNS service. The word "unreachable" in the message indicates the message did not go through to the DNS server. Your browser was not able to obtain the IP address for yummyrecipesforme.com, which it needs to access the website because no service was listening on the receiving DNS port as indicated by the ICMP error message "udp port 53 unreachable."
6. The remaining lines in the log indicate that ICMP packets were sent two more times, but the same delivery error was received both times.

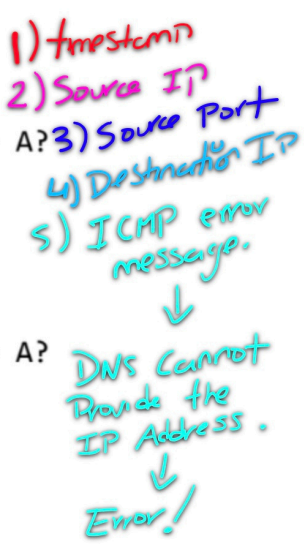
Final Project:

- Detailed Network Packet Examination



```
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
```



- Incident Report:

Example of a
Cybersecurity Incident Repo

This repo **example** is for a di erent security event than the scenario presented in the activity. This example should only be used to familiarize yourself with the expected repo format.

Pa 1: Provide a summary of the problem found in the DNS and ICMP tra c log
The UDP protocol shows that it is not possible to reach the DNS server. As indicated by the outcomes of my network analysis, the ICMP echo reply was an error message “udp po 53 unreachable.” The DNS server commonly uses po 53, but it is unable to nd this po . The DNS server is not responding.

Pa 2: Explain your analysis of the data and provide at least one cause of the incident
The incident occurred today at 1:24 p.m.. Several customers contacted my company to report that they were not able to access the company website “www.yummyrecipesforme.com” These customers said they were getting an error message ~~when trying to load the web page~~ ““destination port unreachable.” Network engineers within the organization are now investigating the issue so our customer can access the website. In my investigation with this issue, I conducted packet sniffing tests using tcpdump. In the results, I saw the issue and it was that port 53 was not able to be reached. Port 53 is commonly used by the DNS server. The next thing to do is check if the DNS server is not working or if the firewall is blocking traffic to port 53. The DNS server might be down because of a successful attack or a setup mistake.

Cybersecurity Incident Report: Network Tra c Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP tra c log.
1. The UDP protocol reveals that: - The UDP protocol reveals that the DNS server is unreachable. **Explanation:** - The UDP protocol analysis indicates that the DNS server cannot be reached, as revealed by an ICMP error message stating the unavailability of UDP port 53. **2. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:** - The ICMP echo reply returned the error message: "udp port 53 is unreachable". **Explanation:** - A er conducting network analysis, it was observed that the ICMP echo reply returned an error message stating that "udp port 53 is unreachable." **3. The port noted in the error message is used for:** - Theport53iscommonlyusedbytheDNSServer. **Explanation:** - The error message speci es port 53, which is the standard port used by DNS servers for communication. **4. The most likely issue is:** - The DNS server cannot translate and provide the IP address for the request from “www.yummyrecipesforme.com” because port 53 is unreachable. **Explanation:** - The primary issue identi ed is that the DNS server cannot ful ll the request for the IP address of "www.yummyrecipesforme.com" because port 53 is unreachable.

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

5. Time incident occurred:

- The incident occurred today at 1 23 p.m..

6. Explain how the IT team became aware of the incident:

- Customers called our organization to notify us that they received an error message “destination port unreachable” when trying to access the website “www.yummyrecipesforme.com”

Explanation:

- Customers alerted our organization by reporting a "destination port unreachable" error when a empting to access the website "www.yummyrecipesforme.com."

7. Explain the actions taken by the IT department to investigate the incident:

- The organization's network security experts are currently looking into the problem a ecting customers. In our investigation, we performed packet sni ng tests using tcpdump. From the resulting log le, we discovered that DNS port 53 was not accessible.

Explanation:

- The IT department, in response to customer reports, initiated an investigation. Packet sni ng tests using tcpdump were performed. The resulting log le revealed the unavailability of DNS port 53.

8. Note key ndings of the IT department's investigation (i.e., details related to the port a ected, DNS server, etc.):

- The incident revolves around UDP port 53, the default port for DNS communication. The ICMP message indicates that the DNS server at 203.0.113.2 cannot be reached on UDP port 53.

Explanation:

- The incident is centered around the DNS server's unavailability on UDP port 53. The ICMP message indicates that communication with the DNS server at 203.0.113.2 on port 53 is not possible.

9. Note a likely cause of the incident:

- DNS server might be down due to a successful Denial of Service a ack or a miscon guration.

Explanation:

- A probable cause of the incident could be the DNS server being down, potentially caused by a successful Denial of Service (DoS) a ack or miscon guration.