Connect and protect

Networks and network security

Activity: Analyze network layer communication

Activity Overview of network and network security course: Connect and protect

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 the 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 in a network and reinforce network security.

Scenario

Review the scenario below.

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.”

13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?

yummyrecipesforme.com. (24)

13:24:36.098564 IP203.0.113.2 > 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 IP203.0.113.2 > 192.51.100.15: ICMP203.0.113.2

udp port 53 unreachable length 320

13:28:32.192571 IP192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?

yummyrecipesforme.com. (24)

13:28:50.022967 IP203.0.113.2 > 192.51.100.15: ICMP203.0.113.2

udp port 53 unreachable length 150

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.

Now that you have captured data packets using a network analyzer tool, it is your job to identify which network protocol and service were impacted by this incident. Then, you will need to write a follow-up report.

As an analyst, you can inspect network traffic and network data to determine what is causing network-related issues during cybersecurity incidents. Later in this course, you will demonstrate how to manage and resolve incidents. For now, you only need to analyze the situation.

In the meantime, this incident is being handled by security engineers after you and other analysts have reported the issue to your direct supervisor.

Analyzing DNS and ICMP traffic in transit using data from a network protocol analyzer tool.

Based on the provided information, it appears that the issue I am investigating involves DNS (Domain Name System) and ICMP (Internet Control Message Protocol) traffic. Let's break down the information.

Customer Complaint:

> Several customers reported that they were unable to access the website www.yummyrecipesforme.com and received the error message "destination port unreachable" when trying to load the page. I also encountered the same issue when trying to access the website.

Network Analyzer tool (tcpdump) Data:

When I loaded my network analyzer tool (tcpdump) and attempted to access the website again, I observed a series of network packets. These packets included UDP packets being sent from my host (192.5.100.15) to a DNS server (203.0.113.2) on port 53, which is the

default port for DNS requests. I received ICMP response from the DNS server with the message “udp port 53 unreachable.”

DNS Request:

My computer (source IP: 192.51.100.15) sent DNS requests to the DNS server (destination IP: 203.0.113.2) using UDP packets. The DNS request was made to resolve the domain name “yummyrecipesforme.com” into an IP address.

ICMP Responses:

In response to my DNS request, the DNS server (203.0.113.2) sent ICMP (Internet Control Message Protocol) responses. These ICMP responses continued the message “udp port 53 unreachable.” The message indicates that the DNS server could not process the UDP packets sent to port 53, which is the well-known port for DNS service.

Packet Analysis:

The DNS packets are DNS requests sent to resolve the domain name www.yummyrecipesforme.com into an IP address. The ICMP responses indicate that the DNS server (203.0.113.2) is returning an error message, especially “undo port 53 unreachable”. This ICMP error message suggests that there is an issue with reaching the DNS server on port 53, which is commonly used for DNS requests.

Protocol and port Information:

The protocol used for communication in this incident was UDP (User Datagram Protocol). The port involved in this incident was port 53, which is associated with DNS service. The term “unreachable” in the ICMP error message further confirms that there was an issue with reaching the DNS service on port 53.

Network Traffic Analysis

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

traffic log.

The UDP protocol reveals that:

UDP (User Datagram Protocol) reveals the following information based on the results of the network analysis in the provided scenario.

Communication Protocol: UDP is a transport layer protocol used for sending data over IP networks. Unlike TCP (Transmission Control Protocol), UDP is connectionless, which means it does not establish a dedicated connection before sending data. It simply sends data packets (datagrams) independently.

Port Number: UDP uses port numbers to identify different services or applications on a network. In the scenario, UDP packets are utilized to send DNS (Domain Name System) queries to resolve the domain name "yummyrecipesforme.com" into an IP address. The source port (e.g., 52444) and destination port (53) are specified in the UDP packets.

DNS Query: UDP packets in the scenario contain DNS queries. These queries are requests to resolve the domain name "yummyrecipesforme.com" into an IP address. This is a typical usage of UDP in DNS resolution, where the DNS server listens on port 53.

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:

This is based on the results of the network analysis, which show:

The network analysis results indicate that there is an issue with DNS (Domain Name System) resolution for the domain "yummyrecipesforme.com." The specific findings from the analysis are as follows:

DNS Request: The network analysis shows the initial outgoing DNS request from your computer to a DNS server. This request is sent using the UDP protocol, and it is aimed at resolving the domain name "yummyrecipesforme.com" into an IP address. The source IP address is your computer (e.g., 192.51.100.15), and the destination IP address is the DNS server (e.g., 203.0.113.2) on port 53.

ICMP Response: Following the DNS request, your computer receives ICMP (Internet Control Message Protocol) responses from the DNS server. These ICMP responses contain the message "udp port 53 unreachable." This message indicates that the DNS server is unreachable on port 53, which is the standard port for DNS service. The length of these ICMP responses varies but includes information about the unreachable port.

Repetition of the Issue: The issue repeats multiple times, with your computer sending DNS queries and receiving ICMP responses with the "udp port 53 unreachable" message. This consistent pattern confirms the problem's persistence. Based on this analysis, it's evident that the DNS protocol over UDP was affected during this incident. The DNS server on port 53 was unreachable, preventing the resolution of the domain name "yummyrecipesforme.com" and resulting in the "destination port unreachable" error.

The port noted in the error message is used for:

The port noted in the error message, which is "udp port 53 unreachable," refers to port 53 and its specific use in the context of the DNS (Domain Name System) protocol.

In networking, port numbers are used to identify specific services or applications running on a device within a network. Port 53 is a well-known and reserved port number that is associated with the DNS service. Specifically, it is used for DNS queries and responses.

Here's what port 53 is used for in the DNS protocol:

DNS Queries: When a client (such as your computer) wants to resolve a domain name (e.g., www.yummyrecipesforme.com) into an IP address, it sends a DNS query to a DNS server. This query is sent to the DNS server's port 53, as specified in the UDP or TCP header of the DNS packet.

DNS Responses: The DNS server listens on port 53 to receive these queries and responds with the corresponding IP address or other DNS-related information. The DNS response is also sent back to the client's port 53.

In the scenario you provided, when your computer sends DNS queries to the DNS server on port 53, it expects to receive DNS responses. However, since the DNS server responds with ICMP messages indicating that port 53 is unreachable, it means that the DNS service on the server is not functioning or reachable on that port. This is why your computer and the customers trying to access the website encounter the "destination port unreachable" error, as the DNS service is not available to perform the necessary domain name resolution.

The most likely issue is:

The most likely issue based on the information provided is that the DNS (Domain Name System) service on the DNS server at IP address 203.0.113.2 is not functioning correctly or is not reachable. Here are the potential root causes of this issue:

DNS Server Unreachable: The ICMP responses indicating "udp port 53 unreachable" suggest that your computer is unable to establish a connection with the DNS server on port 53. This could be due to network issues, such as a firewall blocking traffic to the DNS server or a network misconfiguration that prevents your computer from reaching

DNS server or a network misconfiguration that prevents your computer from reaching the DNS server.

DNS Server Configuration Issue: The DNS server itself might be experiencing problems with its configuration. This could include misconfigured DNS settings, incorrect port configurations, or DNS service errors that prevent it from properly handling DNS queries.

DNS Server Outage: It's possible that the DNS server is temporarily down or experiencing an outage. This could be due to maintenance, hardware failures, or other issues that have taken the DNS service offline.

DNS Server Load: The DNS server might be overwhelmed with DNS queries, causing it to respond slowly or not at all. This could be due to a sudden increase in DNS requests or insufficient resources on the server to handle the volume of requests.

To resolve this issue and restore access to the website www.yummyrecipesforme.com, further investigation and troubleshooting are required. Here are some steps that can be taken to address the problem:

Check DNS Server Status: Verify whether the DNS server at IP address 203.0.113.2 is online and operational. If it's an internal DNS server within your organization, check its status and logs for any errors.

Network Troubleshooting: Examine the network configuration and ensure that there are no network connectivity issues between your computer and the DNS server. Look for firewall rules that might be blocking DNS traffic.

DNS Server Configuration: Review the DNS server's configuration for any errors or misconfigurations. Ensure that it's listening on port 53 and configured to handle DNS queries correctly.

Server Load: If the DNS server is under heavy load, consider load balancing DNS queries across multiple servers or adding additional resources to handle the load.

Temporary DNS Resolution: As a temporary measure, you can configure your computer or your organization's DNS resolver to use an alternative DNS server that is known to be operational, such as a public DNS resolver like Google DNS or OpenDNS.

The specific steps to resolve the issue may vary depending on your organization's network setup and the nature of the problem. It's advisable to involve your network or system administrators to assist in diagnosing and fixing the DNS server issue.

Top of Form

Regenerate

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

Time incident occurred:

The incident occurred at the following times based on the provided log data: The initial DNS request was sent at 13:24:32.192571. The first ICMP response indicating "udp port 53 unreachable" was received at 13:24:36.098564. Subsequent ICMP responses with the same error message were received at 13:27:15.934126 and 13:28:50.022967. The incident started around 13:24 (1:24 PM) and continued with repeated ICMP responses indicating the issue with port 53 on the DNS server. The timestamps are in the format of "HH:MM:SS.ssssss," where HH represents the hour, MM represents the minute, SS represents the second, and ssssss represents microseconds.

Explain how the IT team became aware of the incident:

The IT team became aware of the incident through several means:Customer Reports: Several customers of the company reported that they were unable to access the company website, www.yummyrecipesforme.com. These customers encountered an error message stating "destination port unreachable" when trying to load the website. Customer complaints and reports of website accessibility issues likely triggered the initial

Customer complaints and reports of website accessibility issues likely triggered the initial awareness of the incident.

Employee Experience: The scenario describes that as a cybersecurity analyst working at the company, you also encountered the same error message, "destination port unreachable," when attempting to access the website. This suggests that employees within the organization, including the IT team, experienced the issue firsthand, which further raised awareness of the incident.

Network Traffic Analysis: To investigate and diagnose the issue, the IT team utilized a network protocol analyzer tool, tcpdump. When they attempted to access the website using this tool, they observed a significant amount of network traffic, including DNS and ICMP packets. The analysis of this network traffic revealed the specific error message, "udp port 53 unreachable," which provided insights into the nature of the problem. This network traffic analysis helped the IT team confirm and understand the incident more comprehensively.

In summary, the IT team became aware of the incident due to customer reports, the personal experience of employees encountering the issue, and their proactive use of network analysis tools to investigate the problem further. These factors collectively contributed to their awareness of the incident involving the inaccessibility of www.yummyrecipesforme.com

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

the IT department's investigation involved using a network protocol analyzer tool to capture and analyze network traffic, focusing on DNS and ICMP packets. This analysis led them to identify the root cause of the issue, which was the unavailability of the DNS server on port 53. The investigation provided valuable insights into the incident, allowing them to understand and diagnose the problem.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):

Port Affected: The investigation revealed that port 53 was the port affected by the incident. Specifically, the DNS server at IP address 203.0.113.2 was not

responding on port 53. This was evident from the ICMP response message indicating "udp port 53 unreachable."

DNS Server: The DNS server involved in this incident was located at IP address 203.0.113.2. This server was responsible for handling DNS queries and resolving domain names into IP addresses. However, it was unresponsive on port 53, which is the default port for DNS service

Note a likely cause of the incident:

Top of Form

Bottom of Form

the investigation found that the issue, the cause of the incident was related to the DNS server not responding on port 53, preventing the resolution of domain names and causing the error message "udp port 53 unreachable." This was the root cause of the website inaccessibility.

Issue summary:

The DNS server on 203.0.113.2 was not responding to DNS requests on port 53, preventing the resolution of the domain name “yummyrecipesforme.com” into an IP address. This issue led to the “destination port unreachable” error that I and the customers experienced when trying to access the website.

Conclusion and Finding Issue:

. Based on the information provided, the network protocol affected during this incident is DNS (Domain Name System).

. The ICMP error message “udp port 53 unreachable” indicates that there is a problem With the DNS traffic, and the DNS server on 203.0113.2 is not responding to DNS Requests on port 53, which is essential for resolving domain names.

To solve the issue and restore access to the website, further investigation is needed to Determine why the DNS server is not responding correctly to DNS requests on port 53. Also, further investigation and troubleshooting of the DNS server’s configuration, Network connectivity, and possible or potential firewall or security rules that may be Blocking the DNS traffic is necessary.