Analyze network layer communication

Scenario

You are a cybersecurity analyst working at a company that specializes in providing IT services for clients. Several customers of clients reported that they were not able to access the client 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 attempt to visit the website and you also receive the error “destination port unreachable.” To troubleshoot the issue, you load your network analyzer tool, tcpdump, and attempt to load the webpage again. To load the webpage, your browser sends a query to a DNS server via the UDP protocol to retrieve the IP address for the website's domain name; this is part of the DNS protocol. Your browser then uses this IP address as the destination IP for sending an HTTPS request to the web server to display the webpage The analyzer shows that when you send UDP packets to the DNS server, you receive ICMP packets containing the 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 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
```

Cybersecurity Incident Report:
Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The UDP protocol reveals that: The DNS requests sent from the client to the DNS server using UDP were not successful. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: udp port 53 unreachable. The port noted in the error message is used for: DNS (Domain Name System) services, which resolve domain names to IP addresses. The most likely issue is: The DNS server at IP address 203.0.113.2 is either down, misconfigured, or blocked by a firewall, preventing it from responding to DNS queries on port 53.

Part 2: Explain your analysis of the data and provide at least one cause of the incident
Time incident occurred: the Incident observed multiple timestamps: First one at - 13:24:32.192571, Second one at - 13:26:32.192571, Third one at – 13:28:32.192571. Explain how the IT team became aware of the incident: the IT team became aware of the incident when internal testers and the help desk received multiple reports from customers using alternate communication methods (such as email or phone) indicating they could not access the website www.yummyrecipesforme.com. And state that they encountered a "destination port unreachable" error. Explain the actions taken by the IT department to investigate the incident: the IT department to investigate the incident first is Verified the issue by attempting to access the website and received the same error. Then Utilized the tcpdump network analyzer tool to capture and analyze network traffic during an attempt to access the website. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): 1) These are the findings that found the logs indicated that DNS queries sent from the client's computer (192.51.100.15) to the DNS server (203.0.113.2) were not successful. 2) The DNS queries used the UDP protocol targeting port 53. 3) The DNS server responded with ICMP error messages "udp port 53 unreachable," indicating that port 53 was not accessible on the DNS server. Note a likely cause of the incident: The likely cause of the incident is that the DNS server at IP address 203.0.113.2 is not operational or misconfigured, specifically that the DNS service on port 53 is not running or being blocked by a firewall or access control list.

Summary of the Problem Found in the tcpdump Log
❖ summary of the tcpdump log analysis: The tcpdump log shows repeated DNS queries from the client IP 192.51.100.15 to the DNS server 203.0.113.2, each followed by ICMP "port unreachable" responses. The pattern indicates that the DNS server is rejecting the queries. ❖ These are Identified protocols used for the network traffic: UDP: Used for sending DNS queries from the client to the DNS server. ICMP: Used by the DNS server to respond with "port unreachable" error messages. ❖ Details indicated in the log: Multiple DNS queries for the domain yummyrecipesforme.com. ICMP responses indicating "udp port 53 unreachable." ❖ Interpret the issues found in the log: The log indicates that the DNS server is not accepting queries on UDP port 53, which is preventing clients from resolving the domain name to an IP address. Because of this client unable to access the website.

Analysis of the Data and Solution Implementation

❖ When the problem was first reported:

- The problem was first reported at 13:24:32, according to the tcpdump log.

❖ Scenario, events, and symptoms identified:

- Clients reported being unable to access the websitewww.yummyrecipesforme.com.
- They received an error message indicating "destination port unreachable."
- The IT team confirmed the issue by replicating the error and analyzing the network traffic.Details indicated in the log:

❖ Current status of the issue:

- The log indicates that the DNS server is not accepting queries on UDP port 53, which is preventing clients from resolving the domain name to an IP address. Because of this client unable to access the website.

❖ Information discovered while investigating the issue:

- The DNS server is responding to DNS queries with ICMP "port unreachable" messages.
- The issue is consistent across multiple attempts and times.

❖ Next steps in troubleshooting and resolving the issue:

I. Verify the configuration and operational status of the DNS server at 203.0.113.2.
II. Check for any network issues or firewall settings that might be blocking UDP port 53.
III. Ensure the DNS server software is running correctly and is not misconfigured.
IV. Investigate any recent changes or updates to the DNS server that could have caused this issue.

❖ Suspected root cause of the problem:

- The suspected root cause is a misconfiguration or failure of the DNS server at 203.0.113.2, leading to it rejecting DNS queries on UDP port 53 and responding with ICMP "port unreachable" messages.