Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The network traffic analysis reveals that the UDP protocol encountered an error: "UDP port 53 unreachable." This message was returned by the ICMP echo reply, indicating that the DNS server could not be reached on port 53. **The significance of this port is that it is used for DNS resolution, which translates domain names into IP addresses, allowing users to access websites.** Based on this error, it is clear that the DNS service was not functioning as expected. The most likely issue could be that the DNS server is either down, misconfigured, or has a firewall in place that is blocking requests to port 53. This situation prevented the DNS server from resolving the domain names, which resulted in website access issues for customers.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred around 1:24 p.m., as noted in the tcpdump log timestamps. The IT team first became aware of the problem when several customers reached out, frustrated that they couldn't access the client’s website. They reported receiving a "destination port unreachable" error, which raised immediate concern. To investigate, the IT team replicated the issue by attempting to access the website themselves. They quickly turned to their network analyzer tool, tcpdump, to gather more data. As they tried to load the webpage, their browser sent a DNS query using the UDP protocol to the designated DNS server to obtain the website's IP address. Unfortunately, the analysis

revealed that the DNS request resulted in an ICMP error message stating, "UDP port 53 unreachable." This confirmed that the issue was with the DNS server, as it was not responding to queries directed at it.

The investigation led to suspect a couple of potential causes for the incident. One possibility is that the DNS server might have been misconfigured, preventing it from properly handling requests. Another concern was that a firewall could be blocking access to port 53, which is critical for DNS operations. This blockage would explain why users were unable to resolve domain names and access the website. The team quickly began addressing these possibilities to restore normal service as soon as possible.

Analyze network layer communication

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
```

In the tcpdump log, you find the following information:

1. The first two lines of the log file show 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. The third and fourth lines of the log show the response to your UDP packet. In this case, the ICMP 203.0.113.2 line is the start of the error message indicating that the UDP packet was undeliverable to port 53 of the DNS server.

3. In front of each request and response, you find timestamps that indicate when the incident happened. In the log, this is the first sequence of numbers displayed: 13:24:32.192571. This means the time is 1:24 p.m., 32.192571 seconds.

4. After the timestamps, you will find the source and destination IP addresses. In the first line, where the UDP packet travels from your browser to the DNS server, this information is displayed as: 192.51.100.15 > 203.0.113.2. domain. The IP address to the left of the greater than (>) symbol is the source address, which in this example 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. For the ICMP error response, the source address is 203.0.113.2 and the destination is your computers IP address 192.51.100.15.

5. After the source and destination IP addresses, there can be several additional details like the protocol, port number of the source, and flags. In the first line of the error log, the query identification number appears as: 35084. The plus sign after the query identification number indicates there are flags associated with the UDP message. The "A?" indicates a flag associated with the DNS request for an A record, where an A record maps a domain name to an IP address. The third line displays the protocol of the response message to the browser: "ICMP," which is followed by an ICMP error message.

6. The error message, "UDP port 53 unreachable" is mentioned in the last line. Port 53 is a port for DNS service. The word "unreachable" in the message indicates the UDP message requesting an IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS server because no service was listening on the receiving DNS port.

7. The remaining lines in the log indicate that ICMP packets were sent two more times, but the same delivery error was received both times.