Cybersecurity Incident Report #1: Network Traffic Analysis

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
```

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The UDP protocol reveals that, after sending a query to the DNS server to retrieve the destination website's IP address and then sending an HTTPS request to the web server to access the webpage, users are unable to access the destination website. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: “port 53 is unreachable”. The port noted in the error message is used for DNS service. The most likely issue is that the DNS server is not allowing DNS queries which prevent users from accessing the website.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The first logged incident occurred at 1:24 p.m., 32.192571 seconds. The IT team became aware of this incident after several customers of clients were not able to reach the client company website. When trying to access the website they received the error message: “destination port unreachable”. Following this, the IT department responded by investigating this incident using tcpdump, attempting to access the website, and then analyzing the network traffic. This revealed that the UDP packet sent was undeliverable to port 53 on the DNS server. Since port 53 is unreachable it shows that no service was listening on the receiving DNS port. There could be a few reasons why the DNS server is not allowing DNS queries. Firstly, it could be as a result of a DOS attack, where a threat actor could have over inundated the server with requests causing it to become inactive. It could also be a misconfigured firewall that is blocking UDP traffic to port 53.