Network Traffic 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 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
```

Network Traffic Analysis

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

The logs indicate that port 53 is unreachable when attempting to connect to the website. Port 53 is used for DNS service. This indicates that the UDP message requesting an IP address for the domain did not go through the DNS server because no service was listening on the receiving DNS port. The issue suggests that the DNS service was unavailable—either due to misconfiguration, service outage, firewall restrictions, or a potential malicious disruption such as a denial-of-service attack.

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

The incident occurred around 1:24 pm. Several clients reported that they were not able to access the client company website, and saw the error “destination port unreachable” after waiting for the page to load. The network security responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 53 , which is used for DNS, is not reachable. The logs indicate that ICMP packets were sent multiple times but the same delivery error was received. Potential problems could be DNS service is down, Firewall blocking, or potential Dos/DDos attack.