Cybersecurity Incident Report: 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
```

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.

This event, in the meantime, is being handled by security engineers after you and other analysts have reported the issue to your direct supervisor.

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
Network analysis shows that a UDP request was sent from source IP `192.51.100.15:5244` to destination IP `203.0.113.2` on port 53. However, no successful response was received. Instead, the destination responded with an ICMP echo message indicating a “port unreachable” error. Port

53 is specifically designated for DNS services, and this response suggests that no service was available to process the request. The most likely cause is a missing or misconfigured DNS 'A' record preventing the proper domain-to-IP resolution.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The first failed access attempt occurred at **13:24**, followed by two additional attempts at **13:26** and **13:28**. The IT team was alerted after multiple clients reported they could not access the website: www.yummyrecipesforme.com. In response, the security team conducted three test queries, all of which failed—pointing to a persistent DNS issue. Analysis confirmed that port 53 traffic was not handled properly. A misconfigured or missing 'A' record left the domain unmapped to an IP address, and no service was listening on the destination side to respond. Once the DNS record is corrected and DNS services are verified, access should be restored. It is also recommended to review firewall configurations to ensure legitimate DNS traffic is not inadvertently blocked.