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: to load the webpage, our 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 a part of the DNS protocol. The browser uses an IP address as the destination IP for sending an HTTPS request to the web server to display the webpage. Analyzer shows that when you send UDP packets to the DNS server, you receive ICMP packets containing the error message "udp port 53 unreachable." (Used for DNS). This may indicate that there is a problem going on with the firewall or something like a DDOS attack. The ICMP line is indicating that the UDP packet was undeliverable

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: IMCP 203.0.113.2 udp port 53 unreachable length 254/320 and 150

The port noted in the error message is used for: port 53

The most likely issue is: there is a malicious attack on the firewall or malware attack on web servers like a DDOS attack.

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

Time incident occurred: The first incident was at 13:24:32.192571 ⟶ 1:24

Explain how the IT team became aware of the incident: IT team came aware of the incident due to several customers of clients reporting that they were not able to access the client company website for www.yummyrecipesforme.com, and saw the error error message for port 53 "destination port unreachable" after waiting and page not loading.

Explain the actions taken by the IT department to investigate the incident: The IT department proceeded by loading the network analyzer tool, tcpdump, and attempting to load web page again. In order to load, browser sends a query to a DNS server via the UDP protocol to retrieve IP address. We then use send an HTTPS request to the webserver to display the webpage. In the meantime, security engineers are handling this event after you and other analysts have reported the issue to our direct supervisor.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The IT department found that due to it being “unreachable” in the message meaning that 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

Note a likely cause of the incident: Either a successful DDOS attack or a firewall blocking port 53.