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 DNS is not responding.

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message “udp port 53 unreachable”

The port noted in the error message is used for DNS service.

The most likely issue is the DNS server is not responding after message requesting for IP address for the domain “yummyrecipesforme.com”.

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

Time incident occurred at:

13:24 32.192571

Explain how the IT team became aware of the incident:

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.

Explain the actions taken by the IT department to investigate the incident:

While attempting to access a website, I encountered the error message: “destination port unreachable.” To investigate the issue, I launched our network analysis tool, tcpdump, and retried loading the webpage.

During this process, I observed that the browser initiates a DNS query using the UDP protocol to resolve the domain name to an IP address—standard behavior as part of the DNS resolution process. Once the IP address is retrieved, the browser proceeds to send an HTTPS request to the destination web server in order to render the page.

However, tcpdump revealed that when the UDP packets are sent to the DNS server, the response consists of ICMP packets indicating the error: “udp port 53 unreachable.” This suggests that the DNS server is either not reachable or not accepting traffic on port 53, which is critical for DNS resolution.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):

Accessed the website but received a “destination port unreachable” error. Used tcpdump and found that the browser’s DNS query via UDP failed—ICMP responses indicated “udp port 53 unreachable.” This suggests the DNS server is either down or blocking traffic on port 53.

Note a likely cause of the incident:

Either the DNS server is offline or down after an attack blocking UDP traffic in port 53; port for DNS service.