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: port 53 is unreachable

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: ICMP 203.0.113.2 udp port 53 unreachable

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

The most likely issue is: an ICMP flood attack

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

Time incident occurred: 13.24 - 13.28

Explain how the IT team became aware of the incident: Customers reported they were unable to access the client webpage www.yummyrecipesforme.com. The page would not load and then displayed a message that said “ destination port unreachable “.

Explain the actions taken by the IT department to investigate the incident: First there was an attempt to visit the website , resulting in the error “destination port unreachable.” To troubleshoot the issue they loaded their network analyzer tool, tcpdump, and attempted to load the webpage again. The analyzer showed that when they sent UDP packets to the DNS server, they received ICMP packets containing the error message: “udp port 53 unreachable.”

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The port affected handles DNS requests, and the same error message was received three times.

Note a likely cause of the incident: An ICMP flood attack.