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:
-The client is sending normal DNS requests but the target is replying that the port is closed or not listening.

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 Domain Name System requests

The most likely issue is:
-The DNS service is down, firewalled or deliberately closed.

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

Time incident occurred:
-Between 13:24 and 13:28 local time

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:
-First verified the incident by attempting to access the website with a browser.
- Then a network analyzer tool was used (tcpdump) and attempted to load the webpage again receiving the the info noted in Part 1 UDP port 53 unreachable.

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

-Queries for "yummyrecipesforme.com" consistently failed with “UDP Port 53 unreachable”

-The affected port is UDP 53 which is standard for DNS queries and was reported as unreachable in every ICMP response.

-The DNS server receives packets but has no active listener on port 53 indicating it's not functioning as a DNS resolver.

- No evidence of broader network issues. The problem seems to be isolated to DNS resolution with the target IP responding promptly to indicate the port specific failure.

Note a likely cause of the incident:

-A misconfigured or outdated or inoperative DNS server address.