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 website's domain name resolution wasn't able to be obtained.* **This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:** *UDP port 53 is unreachable.* **The port noted in the error message is used for:** *Obtaining the .domain extension of a website's IP address through a DNS server.* **The most likely issue is:** *Service is down or a possible DoS attack.*

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: *13:24:32 PM* **Explain how the IT team became aware of the incident:** *Several customers reached out stating they had trouble accessing the company's website: www.yummyrecipesforme.com.* **Explain the actions taken by the IT department to investigate the incident:** *The IT team attempted to access the website normally and received a "destination port*

unreachable" error. We then ran a tcpdump to obtain more information and found that UDP Port 53 was unreachable.

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

ICMP packet was undeliverable to the port of the DNS server.
UDP port 53 unreachable.
3 ICMP packets sent total, with none of them reaching the DNS server.

Note a likely cause of the incident:

DNS Service is down, causing port 53 to be unreachable. May indicate a possible DoS attack on the DNS Service.