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: “udp port 53 unreachable” reveals the DNS service on port 53 is unavailable

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

The port noted in the error message is used for: Domain Name System (DNS) port 53

The most likely issue is: An issue with the DNS server

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

Time incident occurred: 1:24 PM

Explain how the IT team became aware of the incident: Customers of clients were unable to access the company website yummyreceipesforme.com

Explain the actions taken by the IT department to investigate the incident: Used a network analyzer tool, tcpdump to troubleshoot the issue

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The logs show ICMP error messages indicate the DNS server could not be reached on port 53. The ICMP error message repeated confirming the issue.

Note a likely cause of the incident: Likely causes is the DNS server being down or a firewall blocking incoming traffic on port 53.