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 UDP protocol reveals that the DNS server is down or unreachable.

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: As evident by the results of the network scan, the ICMP echo reply returned the error message: "udp port 53 unreachable".”

The port noted in the error message is used for: Port 53 is commonly used for DNS protocol traffic.

The most likely issue is: DNS server is not responding.

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

Time incident occurred: 1:24pm

Explain how the IT team became aware of the incident: Several customers contacted your company to report that they were not able to access the company website www.yummyrecipesforme.com,

Explain the actions taken by the IT department to investigate the incident: The network security professionals within the organization are currently investigating the issue so customers can access the website.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): We tried to load the website using a network analyzer tool, tcpdump, and got an error message: “udp port 53 unreachable.”

Note a likely cause of the incident: DNS server might be down due to a successful Denial of Service attack or a misconfiguration.