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: "udp port 53 unreachable" The port noted in the error message is used for: DNS The most likely issue is: A problem with the DNS server. Could be experiencing a DDoS attack.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: The incident occurred at around 1 in the afternoon. 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 Explain the actions taken by the IT department to investigate the incident: Use the network analysis tool tcpdump Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Found that ICMP reply when trying to connect to the website with tcpdump is "UDP port 53 unreachable" Note a likely cause of the incident: This could mean a misconfigured firewall or a Denial of Service attack that is flooding the ports.