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 This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: unreachable The port noted in the error message is used for: DNS servers The most likely issue is:not responding

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 1:23PM Explain how the IT team became aware of the incident: Customers reported the unreachable message when trying to connect Explain the actions taken by the IT department to investigate the incident: Conducting packet sniffing tests using tcpdump Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Found port 53 was unreachable Note a likely cause of the incident: Firewall or DoS attack