Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log
Based on the network analysis findings, it is evident that the DNS server is unresponsive or inaccessible, as indicated by the UDP protocol. The ICMP echo reply generated an error message stating "udp port 53 unreachable," and since port 53 is commonly associated with DNS protocol traffic, it strongly suggests that the DNS server is not providing a response.

Part 2: Explain your analysis of the data and provide one solution to implement
Today, at 1:23 p.m., an incident occurred where customers reported receiving a "destination port unreachable" message when trying to access the website. The IT team was promptly informed by the customers, and network security professionals are currently investigating the issue to restore website accessibility. As part of our investigation, we performed packet sniffing tests using tcpdump. The resulting log file revealed that DNS port 53 was inaccessible. Our next course of action involves determining whether the DNS server is offline or if the firewall is blocking traffic to port 53. It is possible that the DNS server is down due to a successful Denial of Service attack or a misconfiguration.