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 DNS and ICMP traffic log, it is evident that the problem lies with the UDP protocol and specifically port 53. The log shows that when UDP packets are sent to the DNS server, an ICMP response is returned to the host, indicating an error, the error message “UDP port 53 unreachable”. Therefore unable to obtain the IP address for the web server.

Part 2: Explain your analysis of the data and provide one solution to implement
This incident has been brought to the attention of the security team following reports from several customers. In order to investigate, our team first verified the DNS server connectivity ensuring that there were no underlying network connectivity issues. As part of the analysis process, we utilized the network protocol analyzer tool tcpdump to capture and examine any abnormalities or potential causes related to the issue. Additionally, we thoroughly checked the firewall settings on all relevant network devices to confirm that UDP traffic on port 53 was not being blocked. Furthermore, we contacted the system administrator for the web server hosting the website to request a thorough examination for any signs of cyber attacks or suspicious activity. The DNS server might be down due to a successful DoS attack.