Cybersecurity Incident Report: Network Traffic Analysis

Summary of the problem found in the DNS and ICMP traffic log
The network protocol analyzer logs indicate that port 53 is unreachable when attempting to access the website www.yummyrecipiesforme.com. Port 53 is normally used for DNS queries . This may indicate a problem with the DNS configuration. It is possible that this is an indication of a malicious attack on the DNS server.

Part 2: Explain your analysis of the data and provide one solution to implement
The incident first came to my attention this afternoon when several customers contacted the company to report that they were unable to access the website www.yummyrecipiesforme.com. The network security team responded and began running tests with the network analysis tool tcpdump. The results demonstrated that port 53, which is used for DNS queries, was unreachable; the following message displayed “udp port 53 unreachable”,the word “unreachable” indicates the message did not go through the DNS server, the network analysis tool was unable to obtain the IP address for the website because no service was listening. Security engineers took over and are continuing to investigate the root cause of the incident and how to restore normal operations as soon as possible. Our next steps include checking the DNS configuration to check if port 53 is blocked and reporting to the security engineers our findings and if there are any signs of an attack.