Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a 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 DNS server for the domain, www.yummyrecipesforme.com. Port 53 is usually used for the DNS traffic. This may indicate that the DNS service was not available on the destination server, or the firewall rules are blocking access to the DNS server. It could also be due to a DNS attack.

Part 2: Explain your analysis of the data and provide one solution to implement
The incident occurred in the afternoon at 1:24 pm when customers reported that they could not access the “yummy recipe for me” website. The network security team responded and began running tests with the network protocol analyzer tool, tcpdump. The resulting logs revealed that port 53, which is used for DNS traffic, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the DNS server. Our next steps include checking the firewall configurations to see if port 53 is blocked. We are also looking out for signs of a DNS attack and contacting the system administrator for the server to have them check for DNS misconfigurations.