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 www.yummyrecipesforme.com. Port 53 is a well-known port for DNS service. The word “unreachable” in the message indicates the message did not go through to the DNS server. The first log entry shows the DNS request from 192.51.100.15.52444 to 203.0.113.2 asking for the IPv4 address from the domain yummyrecipesforme.com. The second log entry is a ICMP message stating that the IPv4 for yummyrecipesforme.com cannot be reached on port 53. This may be an issue with the firewall or some other network configuration.

Part 2: Explain your analysis of the data and provide one solution to implement
The incident occurred when several customers called this afternoon and reported that they were unable to go on to the company website, yummyrecipesforme.com. The network security team responded and began running tests with the network protocol analyzer tool tcpdump. The ICMP message indicated that the domain of yummyrecipesforme.com was unreachable on port 53, which is used for DNS queries. Upon further investigation, we are indicating that there may be an issue with the firewall configuration blocking traffic or the DNS server is down. Our next steps include firewall configuration to see if port 53 is blocked and contacting the network administrator to see if there are any indications of a DoS attack.