Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The UDP protocol reveals that port 53 was unreachable when attempting to access the website: www.yummyrecipesforme.com This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message port 53 unreachable The port noted in the error message is used for DNS name resolution. The most likely issue is indicative of a misconfiguration of firewall settings or the DNS server itself is configured incorrectly. A malicious attack on the destination web server causing the DNS server itself to crash which would lead to an unreachable port has potential as a cause but is unlikely considering the circumstances

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 1:24 pm Several complaints from customers were reported of not being able to access the yummyrecipesforme.com website due to a “destination port unreachable” error. The issue was reported to the security team and network analysts who are currently working to rectify the issue. The IT department’s investigation used packet sniffing tests and found that port 53 was being blocked from receiving traffic on the yummyrecipes DNS server causing clients attempting to access the server to receive a “destination port unreachable” error. A potential next step is to correct an error in firewall settings denying incoming traffic on port 53 or if the server itself is misconfigured. The DNS server could also be the victim of a DDos attack causing a server crash.