By: caami.sec

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 website www.yummyrecipesforme.com. Port 53 is normally used for DNS traffic. This indicates a problem with the DNS server configuration. The UDP packets sent to request the IP address for the website could not reach the DNS server because no service was listening on port 53.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

The incident occurred today at 1:24 p.m when clients reported that they could not access the website www.yummyrecipesforme.com and received "destination port unreachable" error messages. The IT 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 why the DNS service is not working. Our next steps include checking if the DNS service is running on the server and verifying the server configuration. The IT team suspects that the DNS service may have stopped working or there is a configuration problem that is preventing clients from accessing the website.