Cybersecurity Incident Report

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log

The users were attempting to reach www. yummyrecipesforme.com but no website response was received in their browsers.

TCPDUMP feedback on a user’s computer indicates that the DNS server is not responding to DNS requests on the standard UDP port 53 – this occurred 3 times over 2 minutes. The IP address of the DNS server is reachable, but an ICMP response confirms the lack of DNS response.

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

The incident occurred this afternoon when multiple customers reported they could not reach the www. yummyrecipesforme.com website.

IT used a command-line tool, TCPDUMP, to get additional information on this incident.

The TCPDUMP data indicates the DNS server is reachable, but the DNS service is not responding. Likely, the DNS service needs restarting on this server.