Cybersecurity Incident Report: Network Traffic Analysis

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

The DNS protocol uses UDP to contact the DNS server and retrieve the IP address for the domain name *yummyrecipesforme.com*. In this case, the ICMP protocol returned an error message indicating issues contacting the DNS server. Each log event shows the UDP message from your browser to the DNS server in the first two lines, while the ICMP error response from the DNS server to your browser appears in the third and fourth lines with the message: “udp port 53 unreachable.” Since port 53 is used for DNS traffic, this suggests a problem with the DNS server.

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. Customers reported receiving the message “destination port unreachable” when attempting to visit the website *yummyrecipesforme.com*. The cybersecurity team investigating the issue aims to restore website access for customers. During the investigation, tcpdump packet sniffing tests revealed that DNS port 53 was unreachable. The next step is to determine whether the DNS server is down or if traffic to port 53 is being blocked by a firewall. Possible causes include a successful Denial of Service (DoS) attack or a misconfiguration of the DNS server.