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 was used to contact the DNS server to request the IP address of yummyrecipesforme.com in a UDP packet. The ICMP returned the error message: “udp port 53 unreachable”, indicating that issues communicating with the DNS server. Due to the ICMP error response message about port 53, the most likely issue is that the DNS server is not responding. This assumption is further supported by the flags associated with the outgoing UDP message and domain name retrieval.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred at 1:24 p.m. Several clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load. The IT department investigated the error message by first reproducing the issue and then analyzing network traffic using tcpdump. They observed that DNS queries sent via UDP to port 53 received ICMP error messages stating “udp port 53 unreachable,” indicating that the DNS server was not reachable. As a result, the browser couldn’t resolve the domain name to an IP address, preventing access to the website. The root cause was identified as a failure in the DNS protocol, specifically affecting UDP port 53. The next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall. The DNS server might be down due to a successful Denial of Service attack or a misconfiguration.