Cybersecurity Incident Report:
Network Traffic Analysis

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

As part of the DNS protocol, the UDP protocol reveals that udp port 53 is unreachable when requesting the IP address because no service was listening on the receiving port. Since port 53 is associated with DNS protocol traffic, we know this is an issue with the DNS server. Issues with performing the DNS protocol are further evident because the plus sign after the query identification number 35084 indicates flags with the UDP message and the “A?” symbol indicates flags with performing DNS protocol operations. It is highly likely 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., when several customers of 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. We attempted to visit the website and received the error “destination port unreachable.” To troubleshoot the issue, we used tcpdump, and attempted to load the webpage again. The resulting logs revealed that port 53, which is used for DNS service, is not reachable.

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.