Cybersecurity Incident Report: Network Traffic Analysis

Summary of the Incident
The UDP protocol indicates that port 53 is unreachable. This was determined using a network analyzer tool while attempting to access a client website. When attempting to access the website, the UDP protocol was used to contact the DNS server in an attempt to retrieve the IP address of the website. However, the ICMP protocol responded with an error message stating “udp port 53 log unreachable.” Port 53, as noted in the error message, is a port associated with DNS protocol traffic. It becomes further evident that this is an issue with the DNS protocol due to the existence of a plus sign and “A?” symbol present directly after the query identification number 35084 in the logged response. The existence of the “A?” symbol indicates flags performing DNS operations. This ICMP error message stating that port 53 is not reachable most likely indicates that the DNS server that we are attempting to access is currently not responding.

Analysis of the Incident
The incident occurred at approximately 1:24 p.m. The IT team initially became aware of the incident through reports of customers of a client stating that they were not able to access the client website www.yummyrecipesforme.com. After analyzing the reports of the incident, we attempted to access the client website ourselves and were met with an error message stating “destination port unreachable.” After receiving this error, we again attempted to access the website using the network analyzer tool tcpdump. The resulting logs from the tool indicated that port 53, used for DNS services, is not reachable. The packet was sent an additional two times resulting in the same error message. Since it has been determined that port 53 is currently unreachable, the next steps would be to determine whether the DNS server is down or this issue is being caused by the firewall preventing access to port 53 due to misconfiguration. If the DNS server is indeed down, this may be the result of a DOS attack attempting to prevent access to the client website or other websites by flooding and crashing the server.