Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Summary of the problem found in tcpdump log
As a part of DNS protocol, UDP protocol is used to retrieve the IP address for the domain name of yummyrecipesforme.com. This IP address is used as the destination IP for sending HTTPS request to the web server. The analyzer shows that when UDP packets are sent to the DNS server, ICMP packets containing the error message “udp port 53 unreachable” is received. Port 53 is a port for DNS service. The query identification number appears as: 35084. The plus sign after the query identification number indicates there are flags associated with the UDP message. The “A?” indicates a flag associated with the DNS record for an A record which is mapping a domain name to an IP address. The word “unreachable” in the message indicates the UDP message requesting an IP address for the domain did not go through to the DNS server because no service was listening on the receiving DNS port.

Part 2: Analysis of Data and expected cause of the incident
The incident occurred today at 1:24 p.m. Several customers reported that they were not able to access the company website “www.yummyrecipesforme.com” and received the error as “destination port unreachable”. The Cybersecurity team is currently investigating the incident so that customers can access the website again. In our investigation, we found out that port 53 is unreachable using a packet sniffing tool, tcpdump. Our next step is to find whether the traffic of port 53 is blocked by firewall or the DNS server is experiencing a downtime. It may be possible that DNS server is down due to a Denial of Service attack (DOS) by a threat actor.