Problem found in the DNS and ICMP traffic log

In the scenario given, the UDP protocol indicates that port 53 is unreachable when attempting to access the domain (203.0.113.2.domain). This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: ”udp port 53 unreachable length ’x’”. Port 53 is generally used for DNS (protocol udp/tcp) traffic. The most basic root cause for this issue may be a poorly configured DNS server or server maintenance. It is also possible that this is an indication of a DDoS attack where the DNS server is being flooded with traffic, making it unresponsive.

Analysis & Cause of incident

This incident occurred earlier today when many customers contacted Customer Support concerning the inability to access the webpage www.yummyrecipiesforme.com. The IT department was made aware of this issue and performed a network protocol analysis using the tool tcpdump. The dump returned three connection attempts at 13:24 PM, 13:26 PM, and 13:28 PM. The returned logs demonstrated an inability to establish a connection with the DNS server on port 53. We are currently working on investigating the root cause of this issue so that we can restore access to the public. Our first step is to check the status of the DNS server to see if there is some unannounced maintenance happening, or if the server has been configured correctly. If the server appears to be overloaded, and thus unable to respond to connection attempts, we will attempt to restart the server to reestablish connection. The network security team suspects this is a person attempting to restrict users from accessing the site by means of a DDoS attack. We will do our best to get the server running again and will be performing an investigation to identify the attacker and the cause of the attack.