Incident Report: Submitted by Junior Soc Analyst M.Murtaza
Network Traffic Analysis

Summary of the Problem occurred

The UDP protocol reveals that:
DNS queries sent to the DNS server (203.0.113.2) via UDP port 53 did not receive a valid DNS response. Instead, ICMP error messages were returned, indicating that the DNS service is not reachable on the expected port.
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

The port noted in the error message is used for:
Domain Name System (DNS) services. Port 53 is the standard port used for resolving domain names into IP addresses via the UDP protocol.

The most likely issue is:
The DNS server at IP address 203.0.113.2 is not responding on UDP port 53. This could be due to the DNS service being down, a misconfiguration, firewall blocking UDP traffic on port 53, or the DNS server being decommissioned.

Analysis of the data and possible cause of the incident.

Time incident occurred: 1:24:32 PM, by the tcpdump timestamp 13:24:32.192571.

How the IT team became aware of the incident: Multiple customers reported they were unable to access the client's website www.yummyrecipesforme.com and encountered the error "destination port unreachable." Upon investigation, internal testing by the IT team reproduced the same issue.

Actions taken by the IT department to investigate the incident: The team attempted to load the website and confirmed the issue. They used tcpdump to capture network traffic during the DNS resolution process. Analyzed the captured packets, noting the DNS query sent over UDP and the ICMP "port unreachable" responses**.**

Key findings of the IT department's investigation : UDP requests were sent to DNS server 203.0.113.2 on port 53.ICMP responses indicated udp port 53 unreachable. This confirms that the DNS server is not accepting or responding to queries on its DNS port. This failure prevents domain resolution, which in turn prevents HTTPS communication with the target website.

Note a likely cause of the incident: The DNS server at IP address 203.0.113.2 is either down, misconfigured, or blocked by a firewall. It is not currently providing DNS resolution services on port 53 (UDP), which is critical for domain name resolution.