Incident

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.

Objective

To troubleshoot the issue, you load your network analyzer tool, tcpdump, and attempt to load the webpage again. To load the webpage, your browser sends a query to a DNS server via the UDP protocol to retrieve the IP address for the website's domain name; this is part of the DNS protocol. Your browser then uses this IP address as the destination IP for sending an HTTPS request to the web server to display the webpage The analyzer shows that when you send UDP packets to the DNS server, you receive ICMP packets containing the error message: “udp port 53 unreachable.”

```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```

Report

Summary of the incident
The UDP packet shows that a request was sent to a DNS server with the Ip 203.0.113.2 asking for the corresponding Ip address for the yummyrecipesforme domain using port 53. However, the ICMP echo replied that port 53 is unreachable which is the port responsible for the DNS protocol. It is most likely that the DNS server used is down as there was no port listening on the server

Analysis of the data and a probable cause of the incident.
Time incident occurred: 1:24 p.m., 32.192571 seconds The IT team became aware of the incident as it was reported by several customers and then was confirmed by the team A member of the IT team started testing the problem while running a packet analyzer to see the exact traffic being sent and received which confirmed that port 53 on the server Ip 203.0.113.2 was down thus no customer was able to access this domain. One likely cause of the incident could be a DDOS attack on the server which led to server crashing or becoming unresponsive