Cybersecurity Incident Report:
Analyzing Network traffic

Am working in a company that specializes in IT service for clients. I got several reports from clients that they were not able to access the client company website: www.yummyrecipeforme.com. So I analysed the situation to determine which network protocol was affected. First I attempted to visit the website, then I received the error “destination port unreachable”. So I used the network analyzer Tcpdump, to load the website and then the analyzer showed that when I send UDP packets to the DNS server I received ICMP packet containing error messages

```
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
```

Providing a summary of the problem found in the DNS and ICMP traffic log.
The UDP protocol reveals the packet was undeliverable to Port 53 of the DNS server, after using the tcpdump to analyze the situation. This is based on the result obtained after using the network protocol analyzer, which shows that the ICMP echo reply returned the error message that the “UDP port 53 unreachable”, which the port noted in the error message is used for DNS service. This issue is as a result of packets of ICMP that flooded the server

Explaining my analysis of the data and providing the cause of the incident.
This incident occurred as a 1:24 PM We became aware of the situation after several customers reported that they were not able to access the client company website www.yummyreciepeforme.com, and saw the error “destination port unreachable” after waiting for the page to load. As a cybersecurity analyst I started by attempting to visit the website and I received the error “destination port unreachable” So I troubleshooted the issue using my network protocol analyzer which is the Tcpdump and attempted to load the website again. The browser sent a query to the DNS server via the UDP protocol to retrieve the IP address for the website’s domain name. The browser then uses the IP address as a destination IP for sending an HTTPs request to the web server to display the webpage. The tcpdump shows that when I send a UDP packet to the DNS server , I receive an ICMP packet containing the error message “udp port 53 unreachable”. The likely cause of this incident might be because of the Denial of service attack (DOS)