Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The UDP protocol reveals that, it was used to request a domain name resolution using the address of the DNS server over port 53. 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 relaying requests to yummyrecepiesforme.com by identifying the related IP Address site as it is a DNS port number. The most likely issue is Distributed Denial of Service attack or maybe Network Misconfiguration.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 01:24:32.192571 PM. Explain how the IT team became aware of the incident: Several customers contacted my company to report that they were not able to access the company website www.yummyrecipesforme.com and saw the error “destination port unreachable” after waiting for the page to load. Explain the actions taken by the IT department to investigate the incident: To start, I visit the website, and you also receive the error “destination port unreachable.” Next, I load my network analyzer tool, tcpdump, and load the webpage again. This generates a lot of network traffic packets and I need to analyze those to troubleshoot the issue. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): 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

Note a likely cause of the incident: Maybe a lot of requests overloaded the server so, all the requests cannot be responded to.