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: the UDP protocol was used to request a domain name resolution using the address of the DNS server over port 53. Port 53, which aligns to the .domain extension in 203.0.113.2.domain, is a well-known port for DNS service. The word "unreachable" in the message indicates the message did not go through to the DNS server. Your browser was not able to obtain the IP address for yummyrecipesforme.com, which it needs to access the website because no service was listening on the receiving DNS port as indicated by the ICMP error message "udp port 53 unreachable."

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: requests information from the DNS server and the server replies with the information on the same port.

The most likely issue is: no service was listening on the receiving DNS port

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

Time incident occurred: 13:24:32

Explain how the IT team became aware of the incident: everal customers contacted your 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: sent UDP requests and got an ICMP message after running it on a network packet analyzer tool tcpdump it returned the error that port 53 was unreachable.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): port 53 was unreachable, which means it is not responding

Note a likely cause of the incident: a DoS attach that made the server crash or becomeunresponsive.