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: port 53 is 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: DNS service

The most likely issue is: DDoS attack

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: several customers of clients reported that they were not able to access the client company website 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: attempt to visit the website
performed a network analysis using tcpdump and attempt to load the webpage again

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): when UDP packets are sent to the DNS server, ICMP packets containing the error message “udp port 53 unreachable” are received

Note a likely cause of the incident: the DNS server is flooded with requests which determined the overwhelming of the system and the shut down of the DNS service.