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 52 (DNS Service) 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 52 unreachable length 254

The port noted in the error message is used for: DNS Service

The most likely issue is: The word “unreachable” in the error log indicates that the UDP message requesting an IP address for this domain did not go through to the DNS server because there is no service listening on the receiving DNS port 52.

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

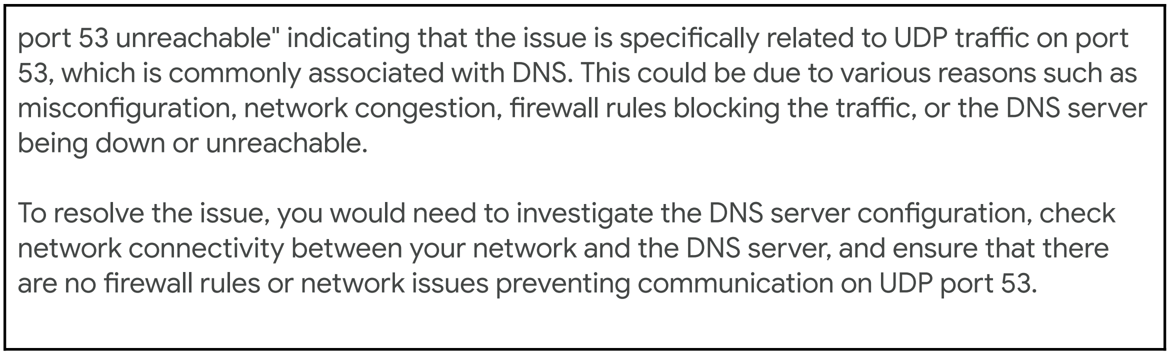
Time incident occurred: As per the log info, the incident first occurred at 13:24 and 32 seconds.

Explain how the IT team became aware of the incident: The IT department first became aware of this incident as several customers had complained they were not able to access the client company website.

Explain the actions taken by the IT department to investigate the incident: To investigate this incident, the IT department checked the tcmpdump log, which is a network analyser tool. Security engineers have taken over and the issue was reported to the direct supervisor.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Key findings are that the incident first occurred at 13:24, it was noted that the UDP statement reported that port 52 was unreachable, and appropriate action was taken by escalating to supervisor and handing over to security engineers.

Note a likely cause of the incident: The ICMP packets containing the error message "udp



port 53 unreachable" indicating that the issue is specifically related to UDP traffic on port 53, which is commonly associated with DNS. This could be due to various reasons such as misconfiguration, network congestion, firewall rules blocking the traffic, or the DNS server being down or unreachable.

To resolve the issue, you would need to investigate the DNS server configuration, check network connectivity between your network and the DNS server, and ensure that there are no firewall rules or network issues preventing communication on UDP port 53.