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: ICMP 203.0.113.2 udp port 53 unreachable length xxx

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

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: 1:24 pm 32.192571 seconds

Explain how the IT team became aware of the incident: Several customers reported the issue.

Explain the actions taken by the IT department to investigate the incident: The team responded and began to run tests with tcpdump a network protocol analyzer.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The team found out that port 53 was unreachable and that it was a DNS service.

Note a likely cause of the incident: No service was listening for the receiving DNS port. Could be from a misconfiguration or a Denial of Service attack.