DNS & ICMP Incident Report

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

The UDP protocol reveals that: A DNS query was made from IP address 192.51.100.15 to the DNS server at 203.0.113.2 requesting the IP for yummyrecipesforme.com using UDP port 53.

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: Port 53 unreachable. This message came from 203.0.113.2, indicating that the DNS server could not process the request.

The port noted in the error message is used for: DNS traffic (UDP port 53), which handles domain name resolution.

The most likely issue is: The DNS service on 203.0.113.2 was either offline, misconfigured, or blocked by a firewall. It could also be the result of a denial-of-service attack targeting the DNS server.

Additional observation: The DNS query log contains flags such as `A?`, which indicates an IPv4 address lookup, and `+`, which suggests DNS query flags were set. These support the assumption that a valid DNS lookup was attempted.

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

Time incident occurred: April 16, 2025 – Beginning at approximately 13:34:22

Explain how the IT team became aware of the incident: Users reported they were unable to access certain websites. The IT department began monitoring the network traffic and ran tcpdump to capture packets.

Explain the actions taken by the IT department to investigate the incident: The team reviewed captured traffic logs and noticed repeated failed DNS queries and corresponding ICMP error responses indicating port 53 was unreachable.

Note key findings of the IT department's investigation: The logs showed that multiple DNS requests to 203.0.113.2 on port 53 failed. The server responded with ICMP messages stating that the port was unreachable. This confirmed that DNS resolution was not functioning correctly for clients.

Note a likely cause of the incident: The DNS server was not responding on UDP port 53. This may be due to the DNS service being down, a misconfiguration in the server or firewall, or a denial-of-service attack that rendered the service unavailable.

Next Steps: The IT team should validate that the DNS service is operational on 203.0.113.2, review system and firewall logs, and apply rate-limiting or DoS mitigation tools if necessary.