⍰ SOC Incident Analysis Template

Incident Title:
DNS Service Unreachable / Port 53 Issue

1. Incident Summary

During network analysis using tcpdump, multiple ICMP “udp port unreachable” messages were observed when the host attempted to communicate with the DNS server via UDP port 53.

2. Evidence / Observation

- Source IP: 192.51.100.15
- Destination IP: 203.0.113.2 (DNS server)
- Protocol: UDP / Port 53
- Response: ICMP “udp port 53 unreachable”
- Behavior: Repeated ICMP responses observed

3. Analysis

The client sent DNS queries to port 53 but received ICMP error responses. Since port 53 is reserved for DNS, this indicates that the DNS service was unreachable or not responding at the time of capture.

4. Possible Causes

- DNS service stopped or crashed
- Firewall blocking UDP port 53
- Network routing or misconfiguration
- DoS/DDoS attack on DNS server causing service unavailability

5. Conclusion / Next Steps

The DNS service was likely unavailable or blocked by a firewall. Next, verify connectivity using ping or nslookup, review firewall rules for port 53, and check DNS server logs for signs of failure or overload.

6. Final Observation / Analyst Note

Based on the evidence, no direct indicators of compromise were found. However, the possibility of a DoS attack or configuration change cannot be ruled out without further investigation.