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: A DNS query was sent from the internal host (192.51.100.15) to the DNS server (203.0.113.2) on port 53, but the server responded with an ICMP error message: "udp port 53 unreachable". This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: "Destination Port Unreachable" The port noted in the error message is used for: The DNS service (standard port UDP/53), which translates domain names (e.g., www.yummyrecipesforme.com) to IP addresses. The most likely issue is: The DNS server (203.0.113.2) is not responding to queries, possibly due to a service outage, misconfiguration, or a denial-of-service attack targeting the DNS infrastructure.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: September 6, 2025, at approximately 13:24:32 UTC (as per tcpdump timestamp: 13:24:32.192571). Explain how the IT team became aware of the incident: Multiple clients reported being unable to access www.yummyrecipesforme.com and received the error "destination port unreachable". The security team reproduced the issue and used tcpdump to capture network traffic, confirming DNS failures. Explain the actions taken by the IT department to investigate the incident: 1. Reproduced the issue by attempting to access the website and observing the error.

2. Captured network traffic using tcpdump during the access attempt.
3. Analyzed the tcpdump log and identified UDP packets (DNS queries) and ICMP error responses.
4. Verified the DNS server status (203.0.113.2) and port 53 accessibility.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):

- Affected Port: UDP port 53 (DNS).
- DNS Server: The authoritative DNS server for the domain (203.0.113.2) is not accepting connections.
- Error Message: ICMP "destination port unreachable" indicates the DNS service is not running or is blocked.
- Source Host: Internal user workstation (192.51.100.15).

Note a likely cause of the incident:
The DNS server (203.0.113.2) may be experiencing a service outage due to:

- A crash or stop of the DNS software (e.g., BIND, Windows DNS).
- A misconfiguration (e.g., firewall rules blocking UDP/53).
- A denial-of-service (DoS) attack overwhelming the server.

Explain the current status of the problem:

The problem is still ongoing. The DNS server remains unresponsive, and users cannot resolve the domain yummyrecipesforme.com.

List the next steps for troubleshooting and resolving the issue:

- Restart the DNS service on the server 203.0.113.2.

- Check firewall configurations to ensure UDP port 53 is allowed.

- Monitor network traffic for signs of DDoS attacks.
- Verify DNS server logs for errors or misconfigurations.