Cybersecurity Incident Report: Network Traffic Analysis

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

The tcpdump analysis reveals that UDP traffic to port 53 (DNS) is failing when attempting to access the client company website, www.yummyrecipesforme.com.

The log shows repeated DNS queries over UDP port 53 from the client (192.51.100.15) to the DNS server (203.0.113.2). Each query receives an ICMP Destination Unreachable – "udp port 53 unreachable" error message. Port 53 is the standard port for DNS services.

This indicates that the UDP DNS request for the domain www.yummyrecipesforme.com did not reach a listening DNS service on the server, possibly due to the DNS service being down, blocked, or overloaded.

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

Time Incident Occurred:
1:24 p.m., 32.192571 seconds (first recorded failure).

How the IT Team Became Aware:
Several customers reported being unable to access www.yummyrecipesforme.com, receiving the error message "destination port unreachable."

Actions Taken by the IT Department:
The IT team used tcpdump to analyze network traffic while attempting to load the webpage.

- The browser first sent a DNS query over UDP port 53 to the DNS server (203.0.113.2) to resolve the IP address.
- No valid DNS responses were received. Instead, the DNS server returned ICMP error packets indicating "udp port 53 unreachable."

Key Findings:

- Protocol Involved: UDP was used for DNS queries, while ICMP was used to return the error messages.
- Issue Observed: DNS resolution failed because the DNS server on port 53 did not respond to queries.

Likely Cause of the Incident:
Based on the evidence, the DNS server for yummyrecipesforme.com is not responding on UDP port 53, possibly due to:

- A misconfiguration or failure of the DNS service.
- A firewall or network policy blocking UDP traffic to port 53.
- A potential Denial of Service (DoS) attack targeting the DNS server, which could have caused the service to go offline or become unresponsive.