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: DNS queries sent from the client computer to the DNS server on port 53 did not go through successfully.

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: ‘udp port 53 unreachable’

The port noted in the error message is used for: DNS (Domain Name System) resolution

The most likely issue is: The DNS was not listening on port 53 of the DNS server, preventing domain names like (www.yummyrecipesforme.com) from being resolved to IP addresses.

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

Time incident occurred: 13:24:32 (1:24 p.m. and 32.192571 seconds, based on tcpdump timestamps).

Explain how the IT team became aware of the incident: Several customers reported they could not access the client’s website and received the error message “destination port unreachable.

Explain the actions taken by the IT department to investigate the incident:

- Analysts attempted to access the site, replicated the error, and ran tcpdump to capture packet data.
- They reviewed DNS queries and ICMP responses for anomalies.

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

- DNS requests from the client computer (192.51.100.15) to the DNS server (203.0.113.2) were blocked.

- The DNS server responded with ICMP error messages indicating **UDP port 53 unreachable**.

- As a result, DNS resolution failed and the web browser could not obtain the IP address of the website.

Note a likely cause of the incident: DNS service outage or misconfiguration on the DNS server (e.g., service stopped, firewall blocking port 53, or DNS server downtime).