Cybersecurity Incident Report:
Network Traffic Analysis

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

The network protocol analyzer logs indicate that UDP port 53 is unreachable when attempting to access the website www.yummyrecipesforme.com. Port 53 is normally used for DNS traffic. This suggests a problem with the DNS server or its configuration. The issue may result from a misconfigured server or a potential network security breach.

The UDP protocol reveals that DNS queries sent from the client to the DNS server did not receive a valid response.

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 service.

The most likely issue is: The DNS server is not available or misconfigured, causing the DNS requests to fail.

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

The incident occurred at the following times:
- 13:24:32.192571
- 13:26:32.192571
- 13:28:32.192571

Explain How the IT Team Became Aware of the Incident
The IT team became aware of the incident after receiving reports from several customers who were unable to access the client company's website www.yummyrecipesforme.com, encountering the error “destination port unreachable.”

Explain the Actions Taken by the IT Department to Investigate the Incident
To investigate the incident, the IT department used the network protocol analyzer tool tcpdump to capture and analyze network traffic. They attempted to access the website, replicated the error, and reviewed the captured logs to identify the root cause of the

problem.

Note Key Findings of the IT Department's Investigation
- The DNS requests sent via UDP protocol to the DNS server (203.0.113.2) from the client’s IP (192.51.100.15) received ICMP error messages indicating that UDP port 53 was unreachable.
- This error occurred consistently across multiple attempts to access the website.
- The DNS server was either not available or there was no service listening on port 53, leading to the failure of the DNS queries.

Note a Likely Cause of the Incident

A likely cause of the incident is that the DNS server (203.0.113.2) is misconfigured or down, resulting in the DNS queries to port 53 being unreachable. This prevented the resolution of the domain name www.yummyrecipesforme.com, causing the website to be inaccessible for users.