Cybersecurity Incident Report:
Network Traffic Analysis

Summary of the Problem Found in the DNS and ICMP Traffic Log

The UDP protocol reveals that:
The UDP protocol is prominently featured in the network analysis, indicating that the DNS (Domain Name System) query for the website www.yummyrecipesforme.com was initiated using UDP packets. UDP is a connectionless transport layer protocol commonly used for lightweight and fast data transmission.

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:
Upon analyzing the network traffic, the ICMP (Internet Control Message Protocol) echo reply delivered an error message in response to the UDP packets sent to the DNS server. The error message specifically stated: "udp port 53 unreachable." ICMP echo replies are typically used for network diagnostics and error reporting.

The port noted in the error message is used for:
The error message indicates that port 53, commonly associated with DNS (Domain Name System) services, was unreachable. Port 53 is the default port for DNS, where DNS servers listen for incoming queries.

The most likely issue is:
The most likely issue identified from the network analysis is that the DNS server, responsible for resolving the IP address associated with www.yummyrecipesforme.com, is not responsive on port 53. This unresponsiveness to the UDP packets sent for DNS resolution is the root cause of the "udp port 53 unreachable" error messages. Possible reasons for this issue include DNS service unavailability, misconfiguration, or firewall restrictions blocking communication on port 53.

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

Time Incident Occurred:
The incident occurred at the timestamp 13:24:32.192571, indicating 1:24 p.m. and 32.192571 seconds.

How the IT Team Became Aware of the Incident:
The IT team became aware of the incident when several customers reported being unable to access the client company website www.yummyrecipesforme.com. Users encountered the error "destination port unreachable" while attempting to load the webpage.

Actions Taken by the IT Department to Investigate the Incident:
Initial Assessment: The IT department initiated an investigation after receiving user reports of website inaccessibility.
Network Analysis: The team employed the use of a network analyzer tool, tcpdump, to capture and inspect data packets related to the attempted access to www.yummyrecipesforme.com.
Observations from tcpdump Log: The tcpdump log revealed issues in the DNS resolution process, with the DNS server responding with "udp port 53 unreachable" errors.
Key Findings of the IT Department's Investigation:
Affected Port: Port 53, associated with DNS services, was identified as the affected port.
DNS Server Unresponsiveness: The DNS server (IP: 203.0.113.2) was unresponsive on port 53, leading to the ICMP error messages.
Likely Cause of the Incident:
The likely cause of the incident is the unresponsiveness of the DNS server on port 53. Possible causes include:

DNS Service Unavailability: The DNS service on the server might be down or experiencing issues.
Misconfiguration: Incorrect DNS server configuration leading to the inability to respond on the specified port.
Firewall Restrictions: Firewall settings might be blocking communication on port 53, preventing the DNS resolution process.