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 client to the DNS server at IP address 203.0.113.2 on port 53. 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, which is essential for resolving domain names to IP addresses. The most likely issue is: that the DNS server is either down, misconfigured, or there is a network issue preventing access to port 53, resulting in the inability to resolve the domain www.yummyrecipesforme.com.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: The incident was first reported at approximately 13:24 PM. Explain how the IT team became aware of the incident: The IT team became aware of the incident when several customers of clients reported that they could not access the website www.yummyrecipesforme.com and received the error message "destination port unreachable." Explain the actions taken by the IT department to investigate the incident: The IT department utilized the network protocol analyzer tool tcpdump to capture and analyze the network traffic related to the DNS queries. They examined the logs to identify any error messages and the status of the DNS server. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The investigation revealed that the DNS query was sent successfully, but the response from the DNS server included an ICMP error indicating that port 53 was unreachable. This suggests that the DNS server at 203.0.113.2 was not

able to process the request.

Note a likely cause of the incident: A likely cause of the incident is that the DNS server is down or misconfigured, preventing it from listening on port 53 and thus failing to respond to DNS queries. Further investigation is needed to confirm the status of the DNS server and any potential network issues.