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: The clients DNS query was sent over UDP to the DNS server on port 53, but it did not receive a valid DNS 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: Port 53, which is a DNS service to resolve domain names to IP addresses The most likely issue is: The DNS server is down, or could be blocked by a firewall, preventing domain resolution.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: The incident occurred at approximately 1:24 p.m., as indicated by the timestamps in the tcpdump log Explain how the IT team became aware of the incident: Customers reported not being able to access the company website www.yummyrecipesforme.com and received "destination port unreachable" errors in their browsers, triggering the IT team's investigation. Explain the actions taken by the IT department to investigate the incident: 1. The IT department attempted to visit the website attempting to replicate the error 2. Collected network traffic using tcpdump during connection attempts 3. Reviewed the captured DNS query and ICMP error messages to pinpoint the cause Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): 1. The DNS query was correctly sent to the DNS server via UDP on port 53 2. The DNS server responded with ICMP "port unreachable" messages confirming the DNS service on port 53 was unavailable

3. Repeated attempts yielded the same ICMP error, ruling out transient network issues

Note a likely cause of the incident: A likely cause of the incident is that the DNS server is unavailable due to either a Denial of Service (DoS) attack overwhelming the server or a misconfiguration (e.g., accidental firewall rule blocking port 53), both of which could prevent the DNS server from responding to legitimate queries.