# 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 UDP protocol reveals that the error message "udp port 53 unreachable" is related to the DNS query being sent over UDP (User Datagram Protocol) on port 53. This suggests that the DNS client is using UDP as the transport protocol to send DNS queries to the DNS server, and the server is not responding or is unreachable on that port.  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 is used for both DNS queries and responses. When a client, such as a web browser, sends a DNS query to a DNS server, it uses port 53. The DNS server then responds with the IP address associated with the domain name, also using port 53.  The most likely issue is:  Based on the analysis of the UDP log, the most likely issue is that the DNS server is not listening on port 53, which is the standard port for DNS service. This is indicated by the error message "udp port 53 unreachable" in the log. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 13:24:32.192571. This means the time is 1:24 p.m., 32.192571 seconds.  Explain how the IT team became aware of the incident: Incident Detection  The IT team became aware of the incident through a combination of monitoring tools and user reports. Specifically, the network analysis revealed the ICMP echo reply error message "udp port 53 unreachable", which indicated a critical issue with DNS resolution. Additionally, users may have reported difficulties accessing certain websites or experiencing slow internet connectivity, prompting the IT team to investigate the issue further. The monitoring tools, such as network performance monitoring software or DNS query logs, likely alerted the IT team to the anomaly in DNS query responses, leading to a deeper investigation and eventual discovery of the issue.  Explain the actions taken by the IT department to investigate the incident:  Initial Assessment: The IT team reviewed the network analysis and monitoring tools to understand the scope of the issue, identifying the error message "udp port 53 unreachable" and its impact on DNS resolution.  DNS Query Analysis: The team analyzed DNS query logs to determine the frequency and pattern of the error, identifying which DNS servers were affected and which clients were experiencing issues.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  Port Affected: UDP port 53, which is the standard port used for DNS queries, was unreachable, indicating a critical issue with DNS resolution.  DNS Server: The investigation revealed that one or more DNS servers were affected, causing the error message "udp port 53 unreachable" and disrupting DNS query responses.  Note a likely cause of the incident: DNS Server Configuration: The investigation found that the DNS server configuration was not the root cause of the issue, as the servers were properly configured and up-to-date. |