# 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 there were attempts to send a query to the DNS server to which resulted in an ICMP message where the UPD port 53 was unreachable.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message “upd port 53 unreachable length 254”.  The port noted in the error message is used for DNS servers and port 53 is the standard port for it.  The most likely issue is the DNS server at 203.0.113.2 IP address is not responding, which could mean the service bring down. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: at 1:24pm as stated in the log as “13:24:32.192571”  Explain how the IT team became aware of the incident: from reports about unable to access the client website and analyzing the ICMP error messages.  Explain the actions taken by the IT department to investigate the incident: using network analyzer tool which in this case using tcpdump and analyzing the traffic and receive ICMP packets.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.) revealed that the DNS server responded on port 53 which was unreachable, and the logs shows repeated attempts to connect but receiving ICMP errors in the end  Note a likely cause of the incident: is that there could be a firewall blocking the port 53 at the DNS server’s address which prevents services from functioning properly |