# 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 was an error when sending a DNS query request  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  The most likely issue is: the client side inbound port 53 is blocked and the DNS server cannot reach the client. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 13:24:32 - 13:28:50  Explain how the IT team became aware of the incident: via several client reports  Explain the actions taken by the IT department to investigate the incident: We first attempted to access the website and confirmed that the website does not load with the error message “destination port unreachable.” Then we reviewed the tcpdump log to further investigate the matter. The cause appears to be the issue with the port 53 which is used for DNS server connections  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): We analyzed the tcpdump log and could verify that the connection from the client to the DNS server was successful with an A record return. However the error message appears when the DNS server tries to send the data back to the client.  Note a likely cause of the incident:  The cause appears to be firewall related. It could be a problem with the physical firewall rule that was altered and blocking the port 53, or a software firewall rule on the OS that is blocking the port. Since it is less likely to have the port 53 blocked from the DNS server side, it is recommended to first check the port 53 on the client devices that are trying to access the website. Be sure to check the inbound IP filter rules of the firewall and ensure that the DNS server IP address is not blocked as well. |