# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log |
| The logs revealed that the DNS server is down or unreachable. This was indicated by the reply of ICMP echo packet which states “UDP port 53 unreachable”. The port 53 is commonly used by DNS servers to handle all the DNS traffic. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide one solution to implement |
| Today at 1:23 pm, we received reports of customers not being able to reach the website and getting the error message “destination port unreachable”. The security team started an investigation to identify the problem and fix this issue immediately. We conducted packet sniffing test using tcpdump, the tests concluded that port 53 is unreachable because the DNS server is down or a misconfigured firewall rule is blocking the port. |