# 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 dns is down or unreachable.  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”. Port 53 is commonly used for DNS protocol traffic.  The most likely issue is: Denial of service attack. The port is being overwhelmed by traffic from most likely threat actors. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident occurred at 1:24 pm. When we were informed by customers complains that they kept on getting “destination port unreachable”. Following the complaints, the security team within the organization started to investigate and used tcpdump to inspect data and found out that port 53 is unreachable, and thus the dns cannot complete the request. The next step is to figure out if the port is blocked by the firewall or if the dns server is down. The dns server might be down due toa successful DoS attack to crash the website or a misconfiguration. |
|  |