# 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: DNS is not responding.  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 Server  The most likely issue is: DNS server is not responding. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 1:24 p.m.  Explain how the IT team became aware of the incident: Several customers of clients reported that they were not able to access the client company website and keep seeing this error “destination port unreachable” after waiting for the page to load.  Explain the actions taken by the IT department to investigate the incident: Security Engineers had to look up on the website and received an error “destination port unreachable”. The team uses tcpdump to analyze traffic to get info about what causing the trouble.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The analyzer shows that when you send UDP packets to the DNS server, you receive ICMP packets containing the error message: “udp port 53 unreachable.”  Note a likely cause of the incident: Dos Attack. The attacker sent the ICMP packet to the DNS server that was causing this error. |