# 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 server 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 unrreachable    The port noted in the error message is used for: dns  The most likely issue is: dns server 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: consumers of the client weren’t able to access site. And informed it team.  Explain the actions taken by the IT department to investigate the incident: Tech tried to connect into url on web broswer to see if error can be repeat . Then I opened terminal and ran tcpdump and collected the log.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): DNS server is either down or port 53 is being blocked by the firewall.  Note a likely cause of the incident: DNS server might be down due to DDOS attack or improper configuration. |