# 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 Server is down or unable to be reached  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 Protocal Traffic  The most likely issue is: server is non responsive | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 1:23PM  Explain how the IT team became aware of the incident: The Customers Called the organization to notify the IT Department of the issue.  Explain the actions taken by the IT department to investigate the incident:The Security team conducted a packet sniffing test using tcpdump.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): the results of the log file indicate that the server is down or traffic to port 53 is blocked by the firewall  Note a likely cause of the incident: the most likly issue that caused this scenario was a DOS attack or Denial of service attack |