# 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 non responsive, when asked for an IP address for a known domain the DNS server failed to respond,**  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: **Communicating with DNS Servers.**  The most likely issue is: **No DNS server was listening on the port** | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: **1:24 PM, 1:26 PM, and 1:28 PM.**  Explain how the IT team became aware of the incident: **Customers complained.**  Explain the actions taken by the IT department to investigate the incident: **The Analyst loaded TCPdump and attempted to connect to the domain. They captured the packets using TCPdump and discovered the error message and underlying problem.**  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): **The IT department discovered that port 53 was non responsive which is the port used to communicate with a DNS Server.**  Note a likely cause of the incident: **The server likely shutdown, it could have lost power, or been overwhelmed by a malicious attack such as a DoS or DDoS attack.** |