# 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: UDP packets sent to the DNS server, an error message is returned.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: udp port 533 unreachable.  The port noted in the error message is used for: DNS  The most likely issue is: The DNS server is either down or misconfigured firewall settings are stopping the connection. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 1:24PM  Explain how the IT team became aware of the incident: Several customers of clients reported that they could not access the website.  Explain the actions taken by the IT department to investigate the incident: Attempted to visit the website and loaded a network analyzer tool to attempt to load the webpage  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Port 53 was found to be unreachable.  Note a likely cause of the incident: DNS server outage or misconfigured firewall. |