# 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:  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:  The port noted in the error message is used for: Domain Name System (DNS) protocol  The most likely issue is: Unable to resolve the IP address for website | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 13.24  Explain how the IT team became aware of the incident: Several customers of clients reported that they were not able to access the client Website  Explain the actions taken by the IT department to investigate the incident:  They tried your network analyzer tool, tcpdump, and attempt to load the webpage again  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  Note a likely cause of the incident: The server is unable to resolve the Website IP address. |