# 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 service is unreachable.  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  The most likely issue is: The DNS service is down. This could be due to a multitude of reasons, including a denial-of-service attack. It could also simply be a non-malicious technical issue with the DNS server. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 1:24 PM  Explain how the IT team became aware of the incident: Customers reported they were unable to access client company website and reported a “destination port unreachable” error.  Explain the actions taken by the IT department to investigate the incident: Ran tcpdump to analyze network traffic to client website.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The DNS service is unreachable, this does not necessarily indicate an issue with our network  Note a likely cause of the incident: Denial-of-service attack against DNS server |