# 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  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: “port 53 is unreachable”  The port noted in the error message is used for: DNS protocol traffic  The most likely issue is: The DNS server is not responding. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred at 1:23 pm  Explain how the IT team became aware of the incident: Customers called the organisation to inform that the website was unreachable and it displayed “destination port unreachable”  Explain the actions taken by the IT department to investigate the incident: They checked the logs using tcpdump  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The DNS server wasn’t responding cause port 53 was unreachable  Note a likely cause of the incident: DOS attack or a misconfiguration |