# 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 findings from the network analysis indicate that the  Dns servers is inaccessible or not functioning  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: this conclusion is supported by by the error message received from the icmp  The port noted in the error message is used for: port 53 is unreachable  The most likely issue is: port 53 is typically associated with dns protocol communication | |
|

| 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: notified by customers that they  Were encountering the destination port is unreachable  Explain the actions taken by the IT department to investigate the incident:  It team is currently engaged in investigating the matter aiming to restore website accessibility for the customers  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): our investigation involved the use of tcpdump for packet sniffing test revealing in the log file that dns port 53 was not accessible  Note a likely cause of the incident: could be a firewall blockage of of port 43 or server itself is experiencing issues |