# 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 or 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 protocol traffic (Port 53)  The most likely issue is that the DNS server is not responding to the request made by the user. | |
|

| 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: customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.  Explain the actions taken by the IT department to investigate the incident: The cybersecurity analyst teams within the organization are investigating the problem using the tcpdump test. In the tcpdump log result, indicating that DNS port 53 was unreachable with an error message “udp port 53 unreachable”, the next step is to determine whether the DNS port 53 is down due to traffic or is being blocked by the firewall.  Note a likely cause of the incident: the DNS server might be down due to DoS attack or due to misconfiguration. |