# 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: port 53 is unreachable when attempting to access yummyreceipesforme.com webpage.  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 length 254  The port noted in the error message is used for: Port 53 is used for both TCP and UDP communication – DNS protocol traffic.  The most likely issue is: It is likely that 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: 1:24 pm  Explain how the IT team became aware of the incident: Several customers reported not being able to access the client company website [www.yummyreceipesforme.com](http://www.yummyreceipesforme.com) and saw the error “destination port unreachable”  Explain the actions taken by the IT department to investigate the incident: launched the network analyzer tool tcpdump  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): When sending UDP packets, the response is an ICMP response  Note a likely cause of the incident: The DNS server might be down from a DoS attack or a misconfiguration with the firewall. |