# 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 the website [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com). The ICMP protocol responds an error message in contacting the DNS server  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, port 53 is for DNS protocol so the issue is with the DNS.  The port noted in the error message is used for: computers to access dns for domain ip address  The most likely issue is: DOS attack is taking place or maybe a misconfiguration |
|

| 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 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: They used tcpdump , a network analyzer tool to load the webpage and the resulting logs revealed that port 53 is unreachable  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The port 53 is affected and the continuous request is redirected or either blocked.  Note a likely cause of the incident: A threat agent might be performing a DOS attack or the service maybe blocked by firewall |