# 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 client company website [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com). This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message “destination port unreachable.” The port noted in the error message is used for DNS protocol traffic. The most likely issue is 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 today at 1:23pm. Several customers 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. The NETWORK SECURITY TEAM is currently investigating the issue so that the customers can access the website again. In our investigation we responded to the incident by first visiting the website and received the same error “destination port unreachable.” After analyzing the network using tcpdump analyzer, the findings showed that port 53 which is for DNS use was not reachable. The most likely cause of the issue is a DoS causing the DNS server to crash or misconfiguration of the firewall blocking port 53. |