# 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. Port 53 is used to communicate with DNS servers.  This may indicate a problem with the web server, and it is possible that this is an indication of a malicious attack on the web server. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident occurred at 1:24 PM, local time, when several customers of our client reported that they were not able to access the client company website [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com). The network security team responded and began an investigative analysis with the network protocol analyzer tcpdump. The resulting logs revealed that port 53, which is used for DNS servers, is not reachable. Further investigation and RCA is underway to determine how access to the website can be restored. As next step, the security team will check the firewall configuration to see if port 53 is blocked and contact the system administrator for the web server to check for any signs of an attack. Based on preliminary findings, the security team suspects this may have been and ICMP DoS attack. |