# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The network protocol analyzer logs indicate that port 53 is unreachable when some customers of client attempting to access the client company website [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com).   Port 53 is normally used for DNS server. This may indicate a problem with the DNS server to translate the IP address that corresponds to the website domain. 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 before 1:00 pm today when 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.*  *The network security team responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 53, which is used for DNS server, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the secure web portal.* |