# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The user’s computer, whose IP address is 192.51.100.15, was not able to reach the website yummyrecipesforme.com because the Domain Name Service (DNS) could not resolve the yummyrecipesforme.com IP address.  The UDP protocol reveals that:  Port 53, used for DNS, was not available/open on the DNS server whose IP address is 203.0.113.2.  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**  The most likely issue is:  The configured DNS server on the user’s computer is not accepting or responding to DNS requests. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred:  This issue was first experienced at 1:24pm, and subsequent requests were experienced at 1:26pm and 1:28pm.  Explain how the IT team became aware of the incident:  The IT Team became aware of this problem when multiple customers reporting they could not access the [www.yummyrecipesform.com](http://www.yummyrecipesform.com) website.  Explain the actions taken by the IT department to investigate the incident:  The IT department was able to replicate the problem from a different source IP address.  A likely cause is that the DNS server’s port 53 for DNS is not open and taking/processing DNS requests. Possibly, the DNS service has failed on the DNS server.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  Note a likely cause of the incident: |