# 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.  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 254.  The port noted in the error message is used for: DNS services  The most likely issue is: a DoS attack. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 1:24 PM, 1:26PM, and 1:28 PM  Explain how the IT team became aware of the incident: Customers couldn't access the website [yummyrecipesforme.com](http://yummyrecipesforme.com). Getting an error message, “destination port unreachable”.  Explain the actions taken by the IT department to investigate the incident: Went to the website themselves to get the same error and used the network analyzer tool, tcpdumb.  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: |