# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| Several customers couldn’t access the site [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com) and saw the error “destination port unreachable.  The UDP protocol reveals that : we receive ICMP packets containing the error message “UDP port 53 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 most likely issue is a DDOS, ICMP Flood, too much ICMP requests sent to the network server. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 1h24 PM or 13:24  Explain how the IT team became aware of the incident : Several customers complained about the fact that they couldn’t reach the site [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com).  Explain the actions taken by the IT department to investigate the incident : look at networks frames when we send a UDP request to the server.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.) : The server won’t respond, “port 53 isn’t reachable”  The most likely cause of the incident is probably an ICMP Flood, which means too much ICMP requests sent to the network server. |