# 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: IP of yummyreciepesform.com is 203.0.113.2 but 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 is unreachable length 254”  The port noted in the error message is used for: Communication between client and DNS servers.  The most likely issue is: ICMP Flood |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 13:24:32.192571  Explain how the IT team became aware of the incident: By the customers saying that they cannot reach the website yummyreceipesform.com  Explain the actions taken by the IT department to investigate the incident: Say to cyber analyst to launch the website with the tcpdump client and look forward to error.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):   * Port 53 is unreachable * UDP message did not go through to the DNS server because no service was listening on the receiving DNS port   Note a likely cause of the incident: A threat send repeatedly ICMP Packet to the DNS. |