# 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 packet can not reach the domain required “yummyrecipesforme.com”  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 53  The most likely issue is “yummyrecipesforme.com” server is offline, or the server is under DoS attack while other users try to access |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 13:24 p.m. while our clients were trying to access to the site.  Explain how the IT team became aware of the incident: the team was notified through tickets  Explain the actions taken by the IT department to investigate the incident: the team started the verification using web browser and displayed “destination port unreachable”, at once tpcdump tool was used. IT department noticed DNS server could not get the yummyrecipesforme.com IP and DNS server returns an error message using ICMP part of the message it was 53 port is affected. Import to say all messages error it was sent immediately after request did.  Note a likely cause of the incident: we believe the error would be cause by DoS attack |