# 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: it’s unable to deliver the request  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: udp port 53 in unreachable  The port noted in the error message is used for: DNS  The most likely issue is: misconfiguration in the firewall, or DDoS attack against the DNS Server. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 13:28:32.192571  Explain how the IT team became aware of the incident: because the ICMP response returned to us, contains the same error messages in the results.  Explain the actions taken by the IT department to investigate the incident: first, checking the timestamps of the response, we see that it takes time to respond to each request.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): our host is trying to ask the DNS server where yummyrecipesforme.com is located, by sending the request through the designated port which is 53. By default, this port should be always available for this kind of requests, but something is blocking it, so it’s probably a firewall. It is also possible that the DNS Server is taking too much time to respond, in that case, the incident must be communicated or escalated to the administrator and check the status of the server, if it’s a DoS attack.  Note a likely cause of the incident: it is probably a misconfiguration of the firewall that is preventing from using the port 53, or a DoS attack against the DNS server. |