# 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:**  The port 53 is unreachable meaning the request to the IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS server because no service was listening on the receiving DNS port.  **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 320"  **The port noted in the error message is used for:**  The port is used for *Domain Name Resolution.*  **The most likely issue is:** Port 53 is commonly subjected to DDoS attacks. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| **Time incident occurred:** 1:24 PM, 1:27 PM, 1:28 PM  **Explain how the IT team became aware of the incident:**  Several customers of clients reported that they were not able to access the client company website “yummyrecipesforme.com” and received the error message “destination port unreachable”  **Explain the actions taken by the IT department to investigate the incident:**  Attempt to visit the website to receive "destination port unreachable". Then troubleshoot the issue by loading the network analyzer tool: tcpdump, and attempt to load the webpage again.  **Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):**  Port 53 is related to Domain Name Resolution for websites. Port 53 is commonly subjected to DDoS attacks.  **Note a likely cause of the incident:**  DDoS attack, firewall configurations black port 53  Solution: Implementing network ingress filtering, Eliminating open DNS resolvers, using random ports instead of port 53. Ensure the network's firewall enabled port 53. |