# 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 UDP packet was undeliverable to port53 of the DNS server when trying to access client company website [www.yummyrecipesforme.com](http://www.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. The port noted in the error message is used for DNS Service. The issue may indicate an issue with the DNS port or a malcious attack. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 13:24:36.098564 (1:24pm)  The IT team became aware of the incident when several custoemrs of theclient reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load. The IT team responded by visting the website and confirming the error message. The IT department then loaded the network analyzer tool, tcpdump, and attempted to load the webpage again. The analyzer shows that when you send UDP packets to the DNS server, you receive ICMP packets containing the error message: “udp port 53 unreachable.” The most likely issue is an ICMP flood, by the attacker sending ICMP packets in large amounts to the server, forcing the servers bandwidth to be taken up due to the server sending packets back. |