# 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 port 53 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. Due to the ICMP error response message about port 53, it is highly likely that the DNS server is not responding. This assumption is further supported by the flags associated with the outgoing UDP message and domain name retrieval. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: (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 next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall. The DNS server might be down due to a successful Denial of Service attack or a misconfiguration. |