# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| Network analysis logs indicate that multiple attempts to connect to the DNS server via UDP requests were detected, which were not answered, suggesting a possible DNS server overload or failure. Analysis of the ICMP traffic revealed an error message of "udp port 53 unreachable", indicating that no service was listening for the receiving DNS port. The port in question, UDP 53, is commonly used for DNS queries. The most likely issue is a DNS service outage, possibly caused by a DDoS attack targeting the DNS server. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident was reported at 1:24 PM when several customers reported difficulty accessing the company's website www.yummyrecipesforme.com, receiving a "destination port unreachable" message after attempting to load the page. The IT team was informed of the issue and began an investigation using the tcpdump network analysis tool to capture and examine DNS and ICMP traffic. The investigation revealed a series of UDP requests to port 53 that received no response from the DNS server, as well as multiple ICMP "Destination Unreachable" responses. It was determined that UDP port 53 on the DNS server was overloaded with excessive traffic, preventing normal responses. The likely cause of the incident was an overloaded DNS server, possibly due to a DDoS attack. |