# 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 attempts to contact the DNS server failed with the error "udp port 53 unreachable." This conclusion 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 protocol traffic. The most likely issue is that the DNS server is not responding. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident occurred today at 1:24 p.m. when customers reported receiving a “destination port unreachable” message while trying to access the website yummyrecipesforme.com. The cybersecurity team, tasked with IT services for the client organization, is investigating the issue to restore website access. As part of the investigation, the team performed packet sniffing tests using tcpdump, which revealed that DNS port 53 was unreachable. The next steps involve determining whether the DNS server is down or if traffic to port 53 is being blocked by the firewall. The downtime could be due to a Denial of Service attack or a misconfiguration of the DNS server. |