# Cybersecurity Incident Report:

# Network Traffic Analysis

| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log | |
| --- | --- |
| At 13:24, there was a DNS query made requesting an A record for “yummyrecipesforme.com”. This happens again at 13:26 and 13:28. The ICMP reply returned “udp port 53 unreachable” each time. Port 53 is commonly used for DNS protocol traffic. This would indicate the DNS server may not be responding. | |
|

| Part 2: Explain your analysis of the data and provide one solution to implement |
| --- |
| Upon analysis of the log and data provided, when customers would attempt to visit the website, they would receive a destination port unreachable message. Network security is currently investigating the issue to determine next steps. Using network logs from tcpdump, it was determined that DNS port 53 was unreachable in requests to the server at 13:24, 13:26, and 13:28. Next steps would be to determine if the DNS server is down or traffic to port 53 is blocked. It is possible that a misconfiguration or Denial of Service attack has occurred and requires further investigation. |