# Cybersecurity Incident Report:

# Network Traffic Analysis

| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. | |
| --- | --- |
| The network protocol analyzer logs indicate that port 53 is unreachable when customers are trying to reach website yummyrecipesforme.com and the page is not loading and be greeted with an error message “destination port unreachable”.  Port 53 is the standard port for DNS and used by both TCP and UDP communication. It’s highly likely 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 happened today at 1:23pm.. Customers called to explain they are unable to reach our website and receive an error message “destination port unreachable”. IT have been informed and the organization's network security professionals are currently investigating this issue so that website is back and running. In our investigation we used TCPdump to conduct a packet sniffing test. In log files it was noticed that it was showing that DNS port 53 was unreachable.  Next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall. DNS server might be down due to an ongoing successful Denial of Service attack or could be a misconfiguration on the DNS server itself. |