# 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 revealed that port 53 is unreachable when attempting to access the company website [www.yummyrecipiesforme.com](http://www.yummyrecipiesforme.com). Port 53 is normally used for DNS protocol traffic. This may indicate that the port is down. It is possible that this is an indication of a malicious attack on the website. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| This incident occurred today at 1:23 pm when the company started receiving several complaints from the customers that the website is down. The network security team responded and began running tests with network protocol analyzer tool tcpdump. The resulting logs revealed that port 53, which is used for TCP/UDP traffic is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the website. Our next steps include checking the firewall configuration to see if port 53 is blocked and checking whether the DNS server is down. This could be a DDoS attack performed against the DNS server or a misconfiguration. |