# Cybersecurity Incident Report:

# Network Traffic Analysis

| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log | |
| --- | --- |
| On 06/05/23 customers contacted support to advise they were not able to access the company website www.yummyrecipesforme.com. ICMP echo revealed that port 53 is unavailable on the DNS server. Port 53 is generally used for DNS requests. There may be a problem with the DNS server or the firewall. This may also be an indication of malicious activity. | |
|

| Part 2: Explain your analysis of the data and provide one solution to implement |
| --- |
| The incident occurred on 06/05/23 at approximately 1323 hrs when several customers reported being unable to access the website. The customers all reported the error, “destination port unreachable.” The network security team ran tests using the protocol analyzer tcpdump. The results indicated that requests to the DNS server on port 53 were not being serviced. Specifically, UDP port 53 was not reachable. We are currently investigating the cause. We are checking the firewall configuration to determine if port 53 is blocked. We will contact the DNS server administrator to ensure the server is configured properly, operational, and not under attack. There is no known cause for the error at this time. |