# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log |
| The DNS and ICMP traffic log indicates that the DNS server is not functioning correctly. The analysis shows that the DNS server is either down or unreachable as evidenced by the ICMP echo returning "udp port 53 unreachable." This points to an issue with the DNS service or server, leading to potential DNS resolution problems and difficulties accessing websites and network resources by their domain names. Further investigation and troubleshooting of the DNS server are required to resolve the problem. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide one solution to implement |
| The data analysis indicates that there is an issue with accessing the company website, [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com/). Both customers and the security team encountered the error message "destination port unreachable" while trying to access the website. To investigate further, the team made a request for the website and received the same error message, confirming the problem. Subsequently, they used tcpdump to capture and analyze the packets sent during the webpage loading process.  The analysis revealed that when they sent UDP packets, they received an ICMP response with the error message "udp port 53 unreachable." This ICMP response indicates that the DNS server, which typically operates on UDP port 53, is down or unreachable. The potential reasons for this unreachability could be due to a misconfiguration in the DNS server settings or, more critically, a successful Denial-of-Service (DoS) attack on the DNS server. A DoS attack overwhelms the server with a flood of traffic, causing it to become unresponsive and unavailable. |