

# 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 report that UDP port 53 is unreachable. when attempting to reach the webpage yummyrecipesforme.com. Exact error message is “udp port 53 unreachable”. This indicates an issue with the DNS server. The DNS server is likely unresponsive.

Part 2: Explain your analysis of the data and provide one solution to implement

Customers contacting our company reported that they were unable to reach the webpage yummyrecipesforme.com. They receive the error “destination port unreachable” when waiting for the page to load. The time of this incident occurring is at 1:24 PM, based on logs. Our network protocol analyzer tool, tcpdump, is showing logs revealing that UDP port 53 is unreachable. Currently, the network team is further investigating the issue to find a solution. It is possible that someone has performed a DoS attack and has succeeded. The next steps would be to check if the DNS server is truly down, or if there is a misconfiguration with the firewall blocking traffic on port 53.