

# Cybersecurity Incident Report:

## Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log

*A user attempted to access the website yummyrecipesforme.com, but was unable to access the website since there was an error with port 53. Port 53 is used for accessing DNS servers, so there may be an issue with the server itself or a malicious attack that is overloading the server.*

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

*The problem was first reported at 1:24 pm by customers. The user made multiple attempts to access the yummyrecipesforme.com website, but was unable to. The user is still not able to access the website. We used tcpdump to analyze the packets, which showed that Port 53 was unreachable. Since Port 53 is commonly used for DNS servers, we should identify which DNS server contains the IP address to yummyrecipesforme.com to see if it is functioning properly, and make sure that network traffic on both the website and the server are as expected. There may be a misconfiguration error, or a successful Denial of Service Attack. We should also check that the firewall between the website and DNS server is functioning properly and not blocking the incorrect information, or being overloaded by unwanted information.*