

# Cybersecurity Incident Report:

## Network Traffic Analysis

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

The tcpdump logs show that the port 53 is unreachable when trying to access the company's website. Port 53 is usually used for Domain Name Service(DNS). This may indicate a problem with the DNS server, maybe a misconfiguration or a DOS attack.

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

The incident was reported at 1:24PM when users tried to visit the site [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com). The IT team received the message as "destination port unreachable". The issue is being reviewed by the team for fixing the problem. Tcpdump was used to sniff the traffic and the logs showed the port 53 was actually unreachable. Our next step is to verify if the DNS server is down or if the firewall is blocking the access. The issue might also have been the result of a successful denial of service attack.