# 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 log indicates that a request was made from the host device with IP 192.51.100.15.52444 to the DNS server with IP 203.0.113.2.domain to resolve the IP address of the destination website yummyrecipesforme.com but the ICMP response UDP port 53 unreachable has been received. This indicates that there may be no device listening on that port or the port could be flooded with an intended malicious UDP requests. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide one solution to implement |
| At 1.23 pm, the customers of yummyrecipesforme.com were trying to access the website but encountered the error saying destination port unreachable. They contacted our cybersecurity firm and upon analyzing the traffic through the network traffic analyzer tcpdump it was found that the port 53 of the DNS server which is responsible for obtaining the IP address of the requested destination was not listening to the request. The ICMP packet was undeliverable to the port of DNS that is why the error message appeared to the user. The root cause of this could be either the port was intentionally/unintentionally closed or maybe the port has had a Dos attack where the port has been flooded with the UDP requests leading to the denial of service to the authentic requests. The system administrator of the DNS server must be asked to further analyze the port and traffic for its unusuality to investigate the reason for why no service is listening to that port so that the server fulfills the user request for the IP address. |