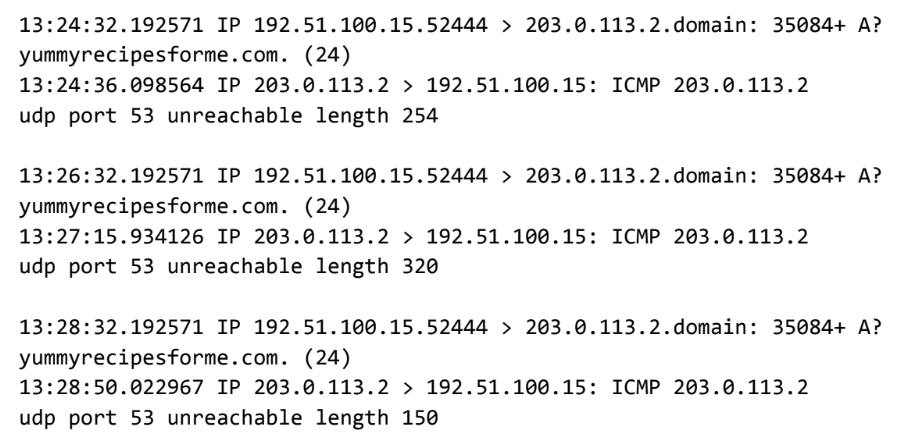
# Cybersecurity Incident Report:

# Network Traffic Analysis



| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. | |
| --- | --- |
| Early in the afternoon multiple customers reported not being able to reach the client’s website www.yummyrecipesforme.com and that they encountered an error when trying to do so. Upon packet sniffer deployment (tcpdump), the team was able to spot through analyzing the ICMP packets that the customers’ DNS requests were not able to reach port 53 on the DNS server side. The mentioned port is mainly used for sending UDP packets to the DNS server. Based on the results of the network analysis, which show that the ICMP echo reply returned the error message ‘udp port 53 unreachable’, we can conclude that there is an ongoing issue with the mentioned port on the server side. One possible reason could be that the DNS server could be under DDoS attack. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| The incident accured in the early afternoon between 1:24pm and 1:32pm. The IT team became aware of the incident through customers’ reports. The team immediately deployed packet sniffers and analyzed the ICMP packets to find out the issue occurred with the port 53 of the DNS server, which was unreachable. Said port is mainly used for sending UDP packets to the DNS server. A likely cause of the incident could be a DDoS attack to the DNS server. |