# Cybersecurity Incident Report:

# Network Traffic Analysis



|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The UDP protocol reveals that the request made for the dns lookup to the dns Ip address(203.0.113,2) for the domain name yummyrecipesforme.com and the dns ip address returned the ICMP error message of UDP port 53 unreachable.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:  The port noted in the error message is used for: DNS Service  The most likely issue is: Most likely this could be an issue of Port 53 being blocked or disabled from web server or it can be the firewall configuration that is blocking the request to port 53 or can be the Network Configuration issue or a successful attack of Flooding the DNS server with the request to perform Denial of service attack |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 13:82:32.192571  Explain how the IT team became aware of the incident: Several customers of the clients reported that they were not able to access the client company website and they saw the error message destination port unreachable.  Explain the actions taken by the IT department to investigate the incident: IT department used the tcpdump network protocol analyzer to analyze the ICMP data packets and attempts to load the website to check the traffic  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): DNS server Ip address :- 203.0.113.2, Port No :- 53 is affected, DNS Server is blocked itself  Note a likely cause of the incident: Most likely this could be an issue of Port 53 being blocked or DNS Server itself is unreachable or is not responding or it can be the firewall configuration that is blocking the request to port 53 or can be the Network Configuration issue. |
| To resolve this issue, firstly we can check the DNS server to see if it is online. If the DNS server is online we can try to check the firewall configuration if it is not blocking the traffic for port 53 and lastly we can check the Network Configuration. |