# 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: Port 53 for DNS service at the destination is inaccessible for the device sending a DNS request.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: “udp port 53 unreachable”  The port noted in the error message is used for: DNS protocols. However, the + after the identification number 35084 indicates that there are flags with the UDP message, and the “A?” symbol indicates flags with DNS protocol operations. Port 34054.  The most likely issue is:  Due to ICMP error response message about port 53, it is highly likely the DNS server is not responding. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 1:24 PM  Explain how the IT team became aware of the incident: Several customers and clients reported they were receiving the error message, “udp port 53 unreachable” while trying to access the website yummyrecipesforme.com  Explain the actions taken by the IT department to investigate the incident: We tried accessing the website ourselves and used tcpdump to look at network activity when we received the same error.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): DNS port 53 was unreachable. We have to identify whether the DNS server is down or traffic to port 53 is blocked by a firewall.  Note a likely cause of the incident: Denial of Service (DoS) attack |