# 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 a UDP packet was sent requesting for the IP address of [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com).  Based on the results of the network analysis, the ICMP reply returned the error message: “UDP port 53 unreachable length 254”, which indicates the DNS server is not responding on port 53.  The port noted in the error message is used for Port 53, which is a standard port used for DNS services  The most likely issue is: The DNS server might either be offline, or overloaded causing it to reject the incoming DNS requests |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 13:24:32.192571 (1:24:32 PM)  The IT team became aware of the incident after several customers reported that they were unable to access the client company’s website ([www.yummyrecipesforme.com](http://www.yummyrecipesforme.com)) and were receiving an error message “Destination Port Unreachable” when attempting to load the page.  Actions taken by the IT department to investigate the incident: The IT team used a network analyzer tcpdump to trace the traffic. When they attempted to access the website, they observed that a UDP packet was sent to the DNS server, to which they received ICMP packets containing the error message “UDP Port 53 unreachable.” This revealed that the DNS server was not responding to the requests.  The Key findings of the IT department's investigation are:  The DNS requests for the domain [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com) were being sent using UDP packets over port 53 which is standard port for DNS service.  The responses from the server were ICMP error messages stating “Destination Port Unreachable.”  Port 53 is a port for DNS service. The word "unreachable" in the message indicates the UDP message requesting an IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS server because no service was listening on the receiving DNS port.  Likely cause of the incident: The DNS server was either down or overloaded by multiples DNS requests (most likely due to a DoS or DDoS attack). This resulted in the server returning ICMP error messages “Destination port unreachable” meaning it could not accept the traffic. |