# 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: show the initial outgoing request from your computer to the DNS server requesting the IP address of yummyrecipesforme.com  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: Is indicating that the UDP packet was undeliverable to port 53 of the DNS server.  The port noted in the error message is used for: is a port for DNS service.  The most likely issue is: 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. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 13:24:32.192571.  Explain how the IT team became aware of the incident: It,s earlier this afternoon Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination UDP port 53 unreachable” after waiting for the page to load.  Explain the actions taken by the IT department to investigate the incident: The network security team  responded and began running tests with the network protocol analyzer tool tcpdump. To load the webpage, the browser sends a query to a DNS server via the UDP protocol to retrieve the IP address for the website's domain name; this is part of the DNS protocol. the browser then uses this IP address as the destination IP for sending an HTTPS request to the web server to display the webpage The analyzer shows that when you send UDP packets to the DNS server, you receive ICMP packets containing the error message: “udp port 53 unreachable.”  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): 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.  Note a likely cause of the incident: The DNS server might be down due to a successful Denial of Service attack or a misconfiguration. |