# 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 DNS server port 53 is unreachable when attempting to access the IP-address of the "www.yummyrecipesforme.com" domain.**  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.**  The most likely issue is:  **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.**  Explain how the IT team became aware of the incident:  **Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com and saw the error “destination port unreachable” after waiting for the page to load.**  Explain the actions taken by the IT department to investigate the incident:  **The network analyzer tool, Tcpdump, was used to troubleshoot the issue, attempts were made to load the webpage by sending a query to the DNS server via the UDP protocol to retrieve the IP address for the website's domain name via DNS protocol.**  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  **The analyzer showed that when UDP packets were sent to the DNS server, ICMP packets containing the error message: “UDP port 53 unreachable” were received.**  Note a likely cause of the incident:  **This may indicate a problem with the DNS server or the firewall configuration. It is possible that this is an indication of a malicious attack on the DNS server.** |