# 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: Receiving error message “destination port unreachable.”  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: The network protocol analyzer logs indicate that port 53 is unreachable.  The port noted in the error message is used for: Communication between a DNS client and a server.  The most likely issue is: no service was listening on the receiving DNS port. This may indicate a problem with the DNS service. It is also possible there is an attempted malicious attack on the DNS service. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: The incident occurred this afternoon, at 1:24 PM.  Explain how the IT team became aware of the incident: Multiple customers reported that they were unable to access the client company website.  Explain the actions taken by the IT department to investigate the incident: Sent ICMP packets at least three times and the same error message displayed each time.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The error message, "udp port 53 unreachable" is mentioned in the last line. 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.  Note a likely cause of the incident: The DNS server is not responding to due blocked firewall port or misconfiguration. |