# 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 indicates that the ICMP packet is not reaching the DNS server, returning the “udp port 53 unreachable” error message, which means the DNS server is unreachable. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| After many clients contacted our company claiming they can’t access the yumyrecipesforme.com website, and getting the error “destination port unreachable”, our team tried the same access and get the same error.  The network security team used the **tcdump** tool for network analysis and load the website again, identifying that when the UDP packet is sent, the ICMP packet returned answer contains the “udp port 53 unreachable” error message, therefore, the packet is not being delivered in this DNS server port.  It is necessary to identify if the DNS server is down or if traffic through port 53 is blocked by the Firewall.  A possible DoS or DDos attack may be in course, but also the chance that there is a misconfiguration in a Firewall is a possibility. |