# 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 UPD packet was not delivered to the DNS server. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: **udp 53 port unreachable.** The port noted in the error message is used for the DNS service. The most likely issue is that the DNS server is unavailable for responding. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident around afternoon, when several customers of client 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. To investigate the incident, we loaded our network analyser (tcpdump) and attempted to load the website again; upon failure to load, we read the generated logs of the network activity.  The sent UDP request attempts to retrieve client website’s IP address from the website’s URL. The DNS server does not respond; instead, the network returns an ICMP error message. The error message clarifies that the DNS server is not listening through port 53, which is designated for the DNS service. In other words, the DNS server is non-operational at the moment. A possible reason was that the server was taken down to stop, recover from and prepare for a DDoS attack.  The issue is reported to our direct supervisor and is being handled by security engineers. |