# 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 IP address cannot be obtained. 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 HTTP traffic. The most likely issue is the server is being overloaded by a potential malicious attack. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| The incident occurred: 1:24 pm when several customers contacted the company reporting they were unable to access the website. The network security team investigated the incident using a network analyzing tool to obtain data packets to uncover the root cause and determine how to restore the web portal. There was no indication that the service was listening on the receiving port causing the error message. The cause of the lack of response is most likely due to a an ICMP Flood attack |