# 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: port 53 of the DNS server is unreachable. In response to the request sent to get the IP address for yummyreceipesforme.com.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: port 53 unreachable  The port noted in the error message is commonly used by DNS server for the request and response for IP address.  The most likely issue is: problem with the DNS server or a DDos attack at DNS server. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: at 1:24pm.  Explain how the IT team became aware of the incident: when customers of the client reported that they were unable to access the client website.  Explain the actions taken by the IT department to investigate the incident: portal. The network security team responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 53, which is used for Requesting IP addresses from DNS servers, is unreachable. We are continuing to investigate the root cause of the issue.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): DNS server is unreachable.  Note a likely cause of the incident: Possible the downtime at DNS server or an attack |