# 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 is inaccessible when attempting to access the yummyrecipesforme.com website  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 length 254  The port noted in the error message is used for: DNS protocol traffic  The most likely issue is: A server crash that is preventing the DNS server from functioning properly thereby not providing the IP Address of the server with website information | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: Earlier this afternoon at 1:22 p.m.  Explain how the IT team became aware of the incident: When several customers contacted the company complaining of their inability to access the yummyrecipesforme.com website  Explain the actions taken by the IT department to investigate the incident: The IT are currently investigating the issue so the customers can access the website again. The Department first tried to access the website and got the same error message stating : udp port 53 unreachable before loading their network analyzer tool tcp dump to load the webpage again  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The tool revealed that port 53 which is used for DNS service was unreachable. We need to identify if the DNS server is down or if traffic to port 53 is blocked by a firewall  Note a likely cause of the incident: we believe a Distributed Denial of Service attack (DDoS) may have caused a crash. And suspect a previous employee that does not want his recipes online any longer |