# 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 DNS server is unable to resolve the target IP address for yummierecipesforme.com on port 53  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: UDP port unreachable  The port noted in the error message is used for: website resolution  The most likely issue is: it appears that the port is not reachable possibly due to it being overloaded by a large quantity of requests | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 13:24:32.192571  Explain how the IT team became aware of the incident: Customers trying to access the website ymmuoerecipiesforme.com reported that the website had become unreachable and displayed an error message stating: destination port unreachable  Explain the actions taken by the IT department to investigate the incident: By deploying a network analysation tool (tcpdump), members of the IT team were able to determine that port 53 was not reachable  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Several additional requests for domain resolution were returned unresolved due to port 53 not being reachable  Note a likely cause of the incident: It appears that port 53 is overloaded with resolution requests possibly linked to a large number of requests. DDos attack is possible |