# 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 port 53 on the DNS server, IP 203.0.113.2, were unreachable at around 13:25 - 13:30. Network analysis results show that the ICMP echo reply returned the error message: “UDP port 53 unreachable”. Port 53 is normally used for DNS services. The issue most likely originated from misconfiguration of a firewall, but it could also indicate a DoS attack. Further research is needed to determine the cause. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| The incident occurred around 13:25, and lasted at least until 13:28, and the IT team was made aware of the incident through customers reporting that they were not able to access the website “www.yummyrecipesforme.com”, the provider of which is a client of our company. Posteriorly the IT team performed network analysis on the issue by trying to connect the the website through sending a DNS request for the aforementioned website domain name to the DNS server. The UDP request and subsequent ICMPresponse were then captured using the tool tcpdump. The incident was likely caused by firewall misconfiguration, which is not likely to be caused by a malicious actor. If the cause is found to be malicious, it is most likely a DoS attack, but confirming either answer requires further research. |