# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log |
| Logs indicate that UDP port 53 is unreachable when connection was attempted as mentioned by the ICMP reply. Port UDP 53 is usually used for DNS traffic and upon some research the result was that if the issue isn’t a result of a firewall misconfiguration then it most probably is a result of a malicious DNS flooding attack technique, but in this case it may be the result of trying to access the domain IP incorrectly. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide one solution to implement |
| The incident occurred on 1:24 PM and 32.192571 seconds, a tcpdump was used to obtain the details regarding the connection failure, if the information provided is correct, then the issue occurred because the port that the IP was trying to access in the domain was an incorrect port as it’s not a number but a string (“domain”) which may have simply been a human sided error on the user’s side, but if that’s not the case then the proper steps would be double checking the firewall configuration and confirm that the DNS port is working as intended, and that there isn’t a virus that replaces the actual port intended for access with a string. |