# 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 unreachable, in real life when I test this I receive NXDomain, which let me know that the domain is not exist  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: The line after we send a request to the DNS, the DNS will reply with a error message  The port noted in the error message is used for: DNS service  The most likely issue is: The domain does not exist in the ISP’s DNS |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: According to the example: 13h24pm, 32.192571s. According to my real-life demo: 01:40am 33.193770  Explain how the IT team became aware of the incident: Let’s say I make a script to auto detect the alert messages.  Explain the actions taken by the IT department to investigate the incident: The analyst will capture this and then notify the team member and security engineer to take an action for this matter.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  Note a likely cause of the incident: Someone in the company try to access a website that the IT department or ISP blocked |

A screenshot of a computer screen

AI-generated content may be incorrect.