# 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 UDP protocol reveals that connection attempt to the service send it the target ip like the IP  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: The service is not allowed, the service is unreachable.  The port noted in the error message is used for: DNS  The most likely issue is:  This port doesn’t allow connection to the computer IP, so it’s possible for DNS attack like DNS service denial. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: This incident occurred at 13:24:32.192571, 13:26:32.192571, 13:28:32.192571  Explain how the IT team became aware of the incident:  The IT team became aware when on the web page the notification is service unreachable and the customer client notified the IT service unavailable.  Explain the actions taken by the IT department to investigate the incident  The IT team when they became aware about that error started to obtain the packets when the incident was generated through the IT team became aware of the problem.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  The port effect is 52444 on the PC, almost 3 attempts to access that DNS service.  Note a likely cause of the incident:  This incident might be caused because the port is not set up correctly or the firewall is blocking the connection to that DNS between the PC and server DNS or some problem related to the network. |