# 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:  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:  The port noted in the error message is used for:  The most likely issue is: |
|

The UDP protocol reveals that currenting the DNS server is currently unreachable, as shown by the network analysis, the ICMP 203.0.113.2 is providing a return error message saying that “UDP port 53 is unreachable.” As a result, the current issue is the DNS Server is not responding.

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred:  Explain how the IT team became aware of the incident:  Explain the actions taken by the IT department to investigate the incident:  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: |

The incident at 1:24pm several customers contacted the company to report to the IT Team that they cannot gain access to the company website and were getting an error “destination port unreachable after waiting for it to load, the network security team is currently investigating the issue to determine what that cause is using tcpdump to capture the data packets as a result of the test we received a IMCP error message that UDP port 53 was un reachable, our next task is to go through the log and determine whether or not the DNS Server is either down or if port 53 is being blocked by the firewall for some reason. after looking at the log is shows that there were 2 other attempts at connecting to the port 53 in quick succession one at 13:26:32 and the other at 13:28:32 suggesting that either the DNS was misconfigured or Denial-of-Service attack (DoS Attack) might have been the source of the problem .