# 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: UDP port 53 ins unreachable  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: 203.0.113.2 udp port 53 unreachable  The port noted in the error message is used for: 53  The most likely issue is: the DNS is down and unreachable |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 1:24 PM, 32 Seconds  Explain how the IT team became aware of the incident: Several customers of clients reported that they were not able to access the client company website and saw the error “destination port unreachable”  Explain the actions taken by the IT department to investigate the incident: To start, they attempted to visit the website and also receive the error “destination port unreachable”. Then next, they load the network analyzer tool, tcpdump and attempted to load the webpage again.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The incident occurred earlier when several customers of the clients reported that they were not able to access the client company website and saw the error “destination port unreachable.” After loading and using the network analyzing tool, we identify that port 53 is unreachable. This port is used for DNS. We are continuing to investigate the root cause of the issue to determine how we can restore access to the website. Our next step includes contacting the system administrator to check the DNS server for any sign of attack.  Note a likely cause of the incident:  It is not likely caused by employees of the company, based on the assessment and descriptions given to us analyst. The possible cause of this either DDoS attack or misconfiguration. |