# 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: Your computer sent DNS requests to the DNS server at IP 203.0.113.2 using UDP port 53. The DNS server responded with ICMP error messages.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: udp port 53 is unreachable  The port noted in the error message is used for: DNS services, specifically for handling DNS queries over UDP.  The most likely issue is:The DNS server at 203.0.113.2 is not accepting Dns requests likely because the DNS service is down or not running on that server. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 13:24:32.192571 (1:24:32 PM) with repeat attempts at 13:26:32 and 13:28:32  Explain how the IT team became aware of the incident: Several users reported being unable to access the website.  Explain the actions taken by the IT department to investigate the incident: The IT team used tcpdump to inspect DNS traffic.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The DNS server IP:203.0.113.2, The destination port: udp port 53  The protocol involved:udp for dns queries and icmp for error reporting,  This happened across three separate time windows.  Note a likely cause of the incident:The DNS server is offline or not running a dns service on port 53. |