# 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 DNS port 53 for address resolution is unreachable. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message (ICMP 203.0.113.2.domain udp port 53 unreachable). The port noted in the error message is used for domain name resolution by the DNS server in this case (203.0.113.2.domain). The most likely issue is the DNS server not responding. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 1:24:32pm. This was due to end users not being able to reach the websites with error message “udp port 53 unreachable”. The security analyst analyzed traffic using a network analyzer tcpdump tool. This indicated domain name server port 53 was unreachable. Firewall configuration from client LAN was checked to see if the port was blocked and when there was no indication of this the server admin was notified to check if any port filtering was implemented and if not, they should check for signs of a DOS attack. |