Cybersecurity Incident Report:

Network Traffic Analysis

| **Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log** | |
| --- | --- |
| The DNS traffic log indicates that the problem lies with the DNS server’s port 53 being unreachable. The ICMP error messages received confirm that UDP packets sent to the DNS server’s port 53 could not be delivered. This problem needs to be addressed on the server side or within the network infrastructure to restore DNS functionality and allow access to the website | |
|

| **Part 2: Explain your analysis of the data and provide at least one cause of the incident** |
| --- |
| The most likely cause of the incident is that the DNS server (or an intermediate device) is blocking or not responding on port 53. This is supported by the ICMP error message "udp port 53 unreachable," which clearly indicates that port 53 on the DNS server is not reachable. Further investigation would involve checking the status of the DNS server, verifying firewall and network settings, and ensuring that the DNS service is properly configured and operational. |