# Cybersecurity Incident Report: Network Traffic Analysis

| Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log |
|---|
| Network protocol analyser logs indicate that port 53 is unreachable when attempting to access the company website. Port 53 is used to request a domain name resolution by using the address of the DNS server over port 53. Could indicate that service is not running as it has been closed, or the firewall is blocking the port. |

| Part 2: Explain your analysis of the data and provide one solution to implement |
|---|
| We received multiple calls from employees having issues today about accessing our company website, and receiving a ‘destination port unreachable’ error. After loading up the website on our end, we received the same error, and then proceeded to run tcpdump and reload the website. This error is occurring because no service is listening on port 53 - the receiving DNS port, which is shown by the ICMP error message. Opening port 53 may be a solution that could solve the issue - firewall could potentially be blocking this service from running. Security engineers are currently working on resolving the incident in the meantime and the root cause. Could also potentially be a DoS attack or misconfiguration. |