

## Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log

The network protocol analyzer logs indicate that udp port 53 is unreachable when attempting to access the company website. Port 53 is a well known port for DNS service. This may be a problem with the DNS server.

Part 2: Explain your analysis of the data and provide one solution to implement

The incident occurred this afternoon when several customers reported that they were not able to access the company website. The network security responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 53, which is used for DNS servers, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the company website. The word unreachable in the message indicates that the message did not go through to the DNS server. The browser was not able to obtain the IP address for the company site, which it needs to access the website. No service was listening on the receiving DNS port as indicated by the error message "udp port 53 unavailable."