

# Cybersecurity Incident Report:

## Network Traffic Analysis

Part 1: Summary of the problem found in the DNS and ICMP traffic log.

The UDP protocol reveals that port 53 is unreachable. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: UDP port 53 unreachable. The port 53 in the error message is used for DNS service. This may indicate a problem with the web server or the firewall configuration. It is possible that this is an indication of a malicious attack on the web server.

Part 2: Analysis of the data and cause of the incident.

The incident occurred earlier this afternoon when the customers of the client company reported that the client company website was inaccessible and also depicted "destination port unreachable" after waiting for the page to load. The network security team responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 53, which is used for DNS service, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the website. Our next steps include checking the firewall configuration to see if port 53 is blocked and contacting the system administrator for the DNS web server to have them check the system for signs of an attack.