# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log |
| Using command line ping to send ICMP packets to the DNS server on port 53 found that the server was unreachable. Port 53 is normally used for UDP traffic. This may indicate a configuration issue with the DNS server or firewall.  It may also indicate a malicious attack on the server. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide one solution to implement |
| Customers reported that they are unable to navigate to the company website reporting “destination port unreachable”. I was able to recreate the problem locally on my browser and confirm seeing the error message. The team ran ping from the command line sending ICMP packets to the DNS server and received an error response for all packets sent: “udp port 53 unreachable”. The DNS server is not listening on port 53 and thus customers are unable to reach the web site / web server by querying DNS to get the IP address. We are looking into the cause of the outage and have communicated the issue to the administrators for the DNS server to look into possible security issues and to check / restore configuration to allow for proper web traffic. |