Cybersecurity Incident Report:
Network Traffic Analysis

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

The UDP protocol reveals connectionless communication was established, with ICMP echo reply showing an error: “UDP Port 53 Unreachable”. Port 53 is used for DNS protocol traffic. This indicates that the issue with website contact is starting at the connection to the DNS server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

A report was taken at 1323 hours when customers contacted us to advise the IT team that they were unable to access our company website, and they received a response stating “destination port unreachable.”

The IT team was immediately advised and are currently investigating the issue. Current phase of action is utilizing a network analyzer tool called tcpdump to intercept data packets to determine the error point. After attempting to connect to the website we received a log file advising that DNS port 53 was unreachable, preventing appropriate traffic direction to our IP.

Initial steps would be to check the DNS server for any signs of attack disrupting normal traffic, or verify DNS server settings for any misconfigurations.