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

traffic log.

The UDP protocol reveals that port 53 is unreachable when attempting to access the company website. This port is usually used for DNS traffic, so there could be a server issue preventing this traffic, possibly the result of a malicious attack. Firewall issues are also possible but less likely given that multiple customers reported the same issue. 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.”

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

The IT team became aware of the incident after multiple customers contacted the company to report that they could not access the company website, receiving "destination port unreachable" error messages after the page failed to load. Upon testing with tcpdump, the team determined that port 53, used for DNS traffic, was not reachable when ICMP request packets received messages in response indicating that port 53 was unavailable. Our next steps will be to investigate both the firewall settings on the company servers as well as check the servers themselves to determine if any security settings have been changed or compromised. It is unclear at this point what may have caused this issue, but the DNS server is implicated as being a point of failure related to this issue.