Cybersecurity Incident Report: Network Traffic Analysis

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

The logs indicate that port 53 is unreachable when attempting to connect to the website. Port 53 is used for DNS service. This indicates that the UDP message requesting an IP address for the domain did not go through the DNS server because no service was listening on the receiving DNS port. The issue suggests that the DNS service was unavailable—either due to misconfiguration, service outage, firewall restrictions, or a potential malicious disruption such as a denial-of-service attack.

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

The incident occurred around 1:24 pm. Several clients reported that they were not able to access the client company website, and saw the error “destination port unreachable” after waiting for the page to load. 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, is not reachable. The logs indicate that ICMP packets were sent multiple times but the same delivery error was received. Potential problems could be DNS service is down, Firewall blocking, or potential Dos/DDos attack.