Cybersecurity Incident Report : Network Traffic Analysis

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

The network protocol analyzer logs indicate that port 53 is unreachable. The ICMP echo reply returned an error message “udp port 53 unreachable.”. Port 53 is normally used for DNS protocol traffic. This may indicate that the DNS server is not responding.

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

The incident occurred around 1:24 pm when the customers contacted the company to report that they were not able to access the company website. 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 traffic, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the secure web portal. Our next steps include checking the DNS server is down or traffic to port 53 is blocked by the firewall. The DNS server might be down due to a successful Denial of Service attack or a misconfiguration.