Cybersecurity Incident Report

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

The UDP protocol shows that the DNS server is unreachable or down. The network protocol analyzer logs reveal that the ICMP echo reply returned the error message “udp port 53 unreachable”. Port 53 is commonly used for DNS protocol traffic, and it is likely that the DNS server is not responding.

Part 2: Explain your analysis of the data and provide one solution to implement

The incident occurred this afternoon at 1:23 p.m. Customers called the organization and notified the IT team they received the message “destination port unreachable” when attempting to visit the website. The incident is currently being investigated by network security professionals within the organization so access to the website is available to customers again. The investigation into the issue was conducted using packet sniffing tests using tcpdump. The resulting log file found that DNS port 53 was unreachable. The next step to troubleshoot the issue is to determine whether 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.