Cybersecurity Incident Report: Network Traffic Analysis

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

I used a packet sniffer, ‘tcpdump’, and loaded the webpage www.yummyrecipesforme.com, again, after receiving complaints. I noticed a lot of packets in the network analyzer. The analyzer shows that when you send UDP packets and receive an ICMP response returned to your host, the results contain an error message: “udp port 53 unreachable.” Port 53 is used for both UDP and TCP communications. This shows that they are some attacks that target vulnerabilities on the DNS server.

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

The incidents occurred about 1:24 pm this afternoon when several customers contacted the company to report that they were not able to access the company website www.yummyrecipesforme.com, and saw the error “Destination port unreachable” after waiting for the page to load. The network security analyst team has responded by running a series of tests with packet sniffers ‘tcpdump’, the resulting logs has shown that port 53 for UDP communications is ’’unreachable’’.

The next step is to identify 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 DoS attack misconfigurations. DNS resolver can be configured to restrict access from external users.