Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the tcpdump log

The DNS protocol is evident where UDP is used to connect to the server and obtain the IP address of the domain yummyrecipesforme.com, the ICMP protocol responds with an error message indicating problems connecting to the server.

The message that the browser sends to the DNS server is displayed in the first two lines of each log event. The third and fourth lines of the log event show the ICMP error response from the DNS server to the browser with the message "udp port 53 unreachable”

Since port 53 is for the DNS protocol, it follows that the problem is with the DNS server.

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

The incident occurred at 1:24 PM, customers reported receiving the message "Destination port unreachable" when trying to access the website yummyrecipesforme.com, during my investigation I performed packet trace tests with tcpdump, in the resulting logs it was detected that port 53 (DNS) was unreachable.

The next step is to check if the DNS server is down, perhaps due to a denial of service attack (DoS), the firewall is blocking traffic to port 53, or if the failure is due to an incorrect configuration.