Cybersecurity Incident Report: Network Traffic Analysis

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

The UDP protocol reveals that port 53 is unreachable,this is based on the results of the network analysis, which show that the ICMP echo reply returned the error message "203.0.113.2 upd port 53 is unreachable"The port 53 noted in the error message is always used for DNS server,the most likely issue is an DOS attack to the DNS server

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

The incident occurred at exactly 13:24:32.192571 this afternoon,the IT team was aware through a report from client that several customers of client can't access client company website www.yummyrecipesforme.com, and they saw error "destination port unreachable" after waiting for page to load. The IT department attempted to visit the website and we also received the error "destination port unreachable", to troubleshoot the issue, we conducted packet sniffing test using tcpdump, and attempted to load the webpage again. To load the webpage, our browser sent a query to a dns server via udp protocol to retrieve the IP address for the website's domain name; this is part of the DNS protocol. Our browser then uses this IP address as the destination IP for sending an HTTPS request to the web server to display the webpage. The analyzer shows that when we send UDP packets to the DNS server, we receive ICMP packets containing the error message: "udp port 53 unreachable." The IT department believes DOS attack was launched on the company website.