Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log
Logs indicate port 53 is unreachable by udp for ICMP traffic, which indicates DNS (domain name system) is down. DNS server did not respond over next several minutes (13:24, 13:26, and 13:28) suggests this is a persistent problem. Possible causes includes DNS server crashed, firewall config problem, or server is suffering from DOS attack through DNS.

Part 2: Explain your analysis of the data and provide one solution to implement
Several customers reported at 13:23 that they were unable to access the website www.yummyrecipesforme.com, error “destination port unreachable”. I confirmed their findings as the website was also unreachable for me. I executed tcpdump and monitored traffic between me and the web server. 3 UDP packets were sent to port 53 (DNS) to determine IP address of website, but no results came back. Three attempts over 5 minutes all failed, pointing at a persistent problem. The fact that all three took extraordinary long time suggests a very congested server, or server is under DOS attack. Our next steps would be to diagnose if the firewall configuration was changed to block port 53 (DNS), check the DNS server’s health status on the web server itself. We can check the SIEM to see if there is an abnormal amount of DNS traffic for the web server. If we are indeed getting DOS attacked, we probably need to engage services like those of CloudFlare, which has a content distribution network to ensure website uptime, and/or running a “hardened” DNS server.