Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The issue preventing access to the client website, www.yummyrecipesforme.com, is related to a failure in the Domain Name System (DNS) service. Specifically, when attempting to resolve the domain name to an IP address, the DNS requests sent via the User Datagram Protocol (UDP) to the DNS server are resulting in an ICMP error response. The error message "udp port 53 unreachable" indicates that the DNS server is not responding to requests on port 53, which is the standard port used for DNS services.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occured this afternoon, at 1:24 p.m., customers reported being unable to access the website www.yummyrecipesforme.com, encountering the error "destination port unreachable." The IT team confirmed the issue and used tcpdump to analyze network traffic. The analysis revealed that DNS requests to the DNS server were met with ICMP error responses stating "udp port 53 unreachable." This indicated that the DNS server was not responding to requests on the standard DNS port 53. The likely causes include the DNS server being down or misconfigured, firewall settings blocking port 53, or a potential Denial of Service (DoS) attack. Further investigation and coordination with network and security teams are needed to identify and resolve the root cause.