Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
Network analysis indicates that port 53, which is used for communication with DNS servers, is unreachable when attempting to access the company website www.yummyrecipesforme.com. This was identified through a UDP probe that triggered an ICMP error message, suggesting that the DNS service is not responding. Since DNS resolution is essential for translating domain names into IP addresses, this issue prevents users from reaching the website. The most likely causes are a misconfiguration in the firewall blocking DNS traffic or a potential malicious attack targeting the DNS server, disrupting its ability to respond to queries.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Earlier this morning, multiple customers reported being unable to access the client company's website, www.yummyrecipesforme.com. In response, the network security team launched an investigation using the network protocol analyzer tool *tcpdump*. Packet sniffing results revealed that port 53, which is essential for DNS communication, was unreachable. This indicates that DNS resolution—the process that translates domain names into IP addresses—was failing. The issue could stem from either a misconfigured firewall blocking DNS traffic or the DNS server being unavailable. Further investigation is needed to determine whether the server is down due to a Denial of Service (DoS) attack or internal misconfiguration.