Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The network protocol analyzer logs indicate that UDP port 53 is unreachable when attempting to send DNS queries to the DNS server at 203.0.113.2. Port 53 is normally used for DNS resolution. Instead of receiving a DNS response, the system receives ICMP messages stating "udp port 53 unreachable." This prevented the browser from resolving the domain name www.yummyrecipesforme.com, which in turn made it impossible to load the website.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred when multiple customers reported that they could not reach the yummyrecipesforme.com website. The security team investigated by capturing network packets using the tcpdump tool. The logs showed that DNS requests sent using UDP to port 53 on the DNS server were not accepted. Instead, the DNS server returned ICMP error messages indicating that the destination port was unreachable. This suggests that the DNS service on the server was not running, that it crashed, or that a firewall/network filter blocked UDP traffic on port 53. Any of these scenarios would prevent DNS resolution, resulting in the website becoming inaccessible. Next steps include checking whether the DNS service on the server is active, verifying firewall rules to ensure port 53 is not being blocked, and examining the server logs to determine whether the DNS process failed due to a misconfiguration or a possible malicious action.