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 UDP requests sent to port 53 of the DNS server (203.0.113.2) are not being processed successfully. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message "udp port 53 unreachable" The port noted in the error message is used for used for resolving domain names to IP addresses -- DNS (Domain Name System) s The most likely issue is that the DNS service on server 203.0.113.2 is not listening on port 53 or is down, preventing the resolution of the domain www.yummyrecipesforme.com and therefore blocking access to the website.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred at 13:24:32.192571 (1:24 PM and 32 seconds) The IT team became aware of the incident because several customers reported that they were unable to access the website www.yummyrecipesforme.com, receiving the error "destination port unreachable" after waiting for the page to load. The IT team used tcpdump (network protocol analyzer) to capture and analyze network traffic while attempting to access the website, thereby identifying the nature of the problem. The key findings of the IT department's are: - Three DNS query attempts were made (at 13:24, 13:26, and 13:28) - All attempts received ICMP error messages "udp port 53 unreachable" - DNS server 203.0.113.2 is not responding to requests on port 53 - The issue prevents domain name resolution to IP address

Possible causes include:

1. The DNS service on server 203.0.113.2 may have crashed or is down
2. A firewall configuration issue blocking port 53
3. A possible DoS (Denial of Service) attack that has made the DNS service unavailable
4. Unplanned maintenance or DNS server malfunction