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: **No UDP messages are being received in port 53 DNS server when we are trying to send the UDP message from my computer.** This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: **ICMP 203.0.113.2** The port noted in the error message is used for: **DNS service (Port 53)** The most likely issue is: **The DNS server being down, the firewall configuration wasn't properly done, and network misconfiguration**

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: **13:24:32.192571 which means 1:24 pm and 32.192571 seconds** Explain how the IT team became aware of the incident: **The IT team became aware of this incident based on customer reports that users were not able to access the website: www.yummyrecipesforme.com** Explain the actions taken by the IT department to investigate the incident: **The IT department has taken different actions to investigate the incident, such as using a network analysis tool TCPdump.** Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): **The key findings the IT department found during their investigation is port 53 not listening/responding with the message "port 53 is unreachable", and that there is a flag in the UDP message** Note a likely cause of the incident: **The reason this incident may have happened may have been that an**

employee tried to restrict users from a specific page, but may have prevented all users from using the website. This could have also happened with a threat actor successfully conducting a DOS attack.