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: That port 53 is not accessable 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: Port 53 is used for DNS service The most likely issue is: The UDP message requesting for an IP address for the domain "www.yummyrecipesforme.com" did not go through the DNS server because no service was listening on the receiving DNS port.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 14:24:32.192571 Explain how the IT team became aware of the incident: Several customers reported that they could not access the company website "www.yummyrecipesforme.com" and saw the error "destination port unreachable" Explain the actions taken by the IT department to investigate the incident: The security analyst first attempted to visit the website and saw the same error the clients get which is cannot access the company website. Then to analyze the situation used a tcpdump to find the root cause of the problem. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The website cannot be accessed due to port 53 being overloaded Note a likely cause of the incident: DDoS is the most likely cause of the incident.