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: The port 53 is unreachable when attempting to access the Yummyrecipesforme.com website 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 a port for DNS service The most likely issue is: It is possible that this is an indication of a malicious attack on the web server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 1:24 pm Explain how the IT team became aware of the incident: Several customers reported that they could not access the website and were given a page that showed an error code of udp port 53 unreachable Explain the actions taken by the IT department to investigate the incident: To identify the problem we attempt to access the website normally and encounter the error that was reported. Then we proceeded to use a TCPdum to analyze the issues causing the error message Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The port 53 is used for the DNS server so its possible a malicious actor is trying to affect the website or that we may have increased traffic that the server can not handle at this time Note a likely cause of the incident: