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: Port 53 is unreachable when attempting to access the DNS server and receive the correct IP address 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: DNS protocol traffic The most likely issue is: An issue with the DNS servers. This could be a DoS attack on DNS servers

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 1:24:32 but was detected by users earlier who couldn't access the website Explain how the IT team became aware of the incident: Users were not able to access the website and saw "destination port unreachable" Explain the actions taken by the IT department to investigate the incident: Used tcpdump when attempting to access the website to analyze the request to DNS and resulting ICMP packet that was returned Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): There is an issue with accessing port 53 which is used by the DNS servers. This is preventing users for getting the correct IP address for our website and being able to access it Note a likely cause of the incident: This incident could be caused by a DoS attack on DNS servers that it overwhelming them with traffic. Or it could potentially be caused by port 53 being blocked by the firewall