Example of a Cybersecurity Incident Report

This report **example** is for a different security event than the scenario presented in the activity. This example should only be used to familiarize yourself with the expected report format.

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log
The tcpdump traffic logs indicate that udp port 53 is unreachable when attempting to access the client company website www.yummyrecipesforme.com. Port 53 is normally configured to be used for DNS traffic. This may indicate a problem with how the web server is configured.

Part 2: Explain your analysis of the data and provide at least one cause of the incident
The incident occured in the afternoon around 1:24 p.m. when customers of clients reported to IT stating that the client company website www.yummyrecipesforme.com was inaccessible, producing the error "destination port unreachable" after waiting for the page to load. To investigate the incident, IT utilized the network analysis tool tcpdump to monitor network traffic as they attempted to access the website themselves. In IT's attempt to establish a connection with the website, a DNS request was sent to the web server and, if received correctly, the web server would respond with its IP address. However, instead, the web server responded with an ICMP error message stating "udp port 53 unreachable." Normally, port 53 is configured to handle DNS, but with port 53 being unreachable this error indicates that DNS was never properly configured on the web server, which caused customers to see the "destination port unreachable" error in the first place.