Cybersecurity Incident Report

Here's my analysis of a possible attack scenario presented as a part of the certification process.

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log
The network protocol analyzer logs indicate that port 53 is unreachable when attempting to access the yummyrecipiesforme.com website. Port 53 is used for the Domain Name System (DNS) service. This may indicate a problem with the DNS server or the network connectivity or the firewall configuration might be blocking access to port 53. The possibility is that it could be a DoS attack or misconfiguration.

Part 2: Explain your analysis of the data and provide one solution to implement
The incident occurred this afternoon at 1:23 p.m., when several customers reported that they could not reach the yummyrecipiesforme.com website and said that they received the message "destination port unreachable". The network security team responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 53, which is used for the DNS server, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the website. Our next steps include checking whether the DNS server is down or not running, or if there is a network connectivity issue between the client and the DNS server, or if the firewall or network configuration is blocking access to port 53 and contacting the system administrator for the webserver to have them check the system for signs of an attack.