Cybersecurity Incident Report: Network Traffic Analysis

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 website. Port 53 is normally used for DNS service. This may indicate a problem with the web server or the firewall configuration. This could be an indication of a malicious attack on the web server.

Part 2: Explain your analysis of the data and provide one solution to implement
The incident occurred around 1:24 p.m when several customers reported that they were not able to access the company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load. 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 DNS service, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the secure web portal. Our next steps include checking the firewall configuration to see if port 53 is blocked or affected by traffic. Meanwhile, this is a possible DoS attack (since the continuation of service/ running of the business was hindered).