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: DNS servers The most likely issue is: A Denial of Service attack has occurred on the DNS server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: at, or before, 1:24 PM in the afternoon. Explain how the IT team became aware of the incident: Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error "destination port unreachable" after waiting for the page to load. Explain the actions taken by the IT department to investigate the incident: The network security team responded by running tests with tcpdump and attempting to load the website to investigate the incident. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The results of the tests were that port 53 (for DNS servers) was unreachable with the request number to the website being extremely high as an indicator of there being an issue. Note a likely cause of the incident: A DoS attack occurred on the port for the DNS server, port 53, and was likely to be flooded with several requests at once, which overloaded the

server.