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 in the website yummyrecipesforme.com with a UDP packet, port 53 is used for DNS which indicates that the browser is not able to reach the DNS server to obtain the IP address. The process was repeated and ICMP packets were sent two more times, but the same delivery error was received both times.This may indicate a problem with the DNS server configuration or malfuntion in the system. It could be down due to a malicious attact |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide one solution to implement |
| The incident occurred today at 1:24 p.m when several customers contacted our company to report that they were not able to access the company website. I started to analyzing the situation and began running tests with the network protocol analyzer tool tcpdump. The resulting logs showed that that port 53 which is used for the DNS service is unreachable and the clients don't have access to the website IP. the incident is being handled by security engineers and they are continuing to investigate the root cause of the issue. the next steps are to verify the status of the DNS server and reboot if it's down and verify if the information of the website it's correct.The network security team suspects that it could be a DOS attack |