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 UDP port 53 is unreachable when attempting to access company website [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com/) ,Port 53 is a well known port for DNS service, So it seems like the request did not go through to the DNS Server. Browsers are not able to obtain IP address of website. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide one solution to implement |
| The incident occured at 1:24 when Several customers contacted to report that they were not able to access company website [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com/) . The network security team responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs reavealed that port 53, which is used for DNS service was unreachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to website. Next step includes checking firewall configuration to see if port 53 is blocked and contacting the security administrator for the dns server to have them check the system for DOS attack |