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 acccess the recipe website [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com/). Port 53 is normally used for DNS queries, translating domain names to an IP address. This may indicate a problem with the DNS server, or the firewall configuation. It is possible that this is an indication of a DDoS or DoS attack. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide one solution to implement |
| The incident occurred earlier this afternoon around 1:23pm and was brought to our attention when several customers contacted our company to report they were not able to access a website at the domain name [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com/). The network security team responded and began running packet sniffing tests with the network protocol analyzer tool tcpdump. The resulting info revealed that port 53, which is used for DNS resolving, is not reachable. This could be due to a misconfigured network, a failure of the DNS server, or a DDoS or DoS attack. We are continuing to investigate the root cause of the issue to determine how we can restore access to the the website. One possible solution to try, if you do not have access to the DNS server, is to temporarily switch to an alternative DNS server, for instange Google Public DNS, Open DNS, or Cloudflare. |