# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The network analyzer logs indicate that “UDP port 53 is unreachable” when attempting to visit the client company website [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com). The port 53 is normally used for DNS service. This may indicate the problem that IP address for the domain [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com) did not go through to the DNS server because no service was listening on the receiving the DNS port. It is possible that this is an indication of malicious attack on the DNS server. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| This incident occurred this afternoon at 1:24 p.m. when the client reported an inability to access their company website. The network security team immediately responded and began testing with the network protocol analyzer tool, tcpdump. The logs indicated that port 53, typically used for DNS services, is unreachable. We are currently investigating the root cause of the issue to determine how to restore access to the client's website. Our next steps involve checking the firewall configuration for potential blocks on port 53 and contacting the web server to investigate any signs of an attack. The client suspects that a customer might be attempting to prevent them from ordering new recipes, and the network security team is considering the possibility that this individual could have launched an attack to disrupt the client's website. |

A screenshot of a computer code

Description automatically generated