# 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: **Port 53 is unreachable when attempting to access the secure employee background check 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: **Request a domain name resolution using the address of the DNS server.**  The most likely issue is:  **The word “unreachable” in the message indicates the message did not go through to the DNS server. Your browser was not able to obtain the IP address for yummyrecipesforme.com, which it needs to access the website because no service was listening on the receiving DNS port as indicated by the ICMP error message “udp port 53 unreachable.”** |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident occurred early this afternoon at **1:24 p.m.** Several customers contacted our company to report that they were not able to access the company website **www.yummyrecipesforme.com** and saw the error **“destination port unreachable”** after waiting for the page to load. To start, we visited the website, and we also received the error **“destination port unreachable.”** And then, loaded our network analyzer tool and loaded the webpage again. This time, we received a lot of packets in your network analyzer. The analyzer shows that when you send UDP packets and receive an ICMP response returned to your host, the results contain an error message: **“udp port 53 unreachable.”** The log indicates that ICMP packets were sent two more times, but the same delivery error was received both times. The HR team believes it is possible that a  certain new hire may want to keep them from performing the background check. The  network security team suspects this person might have launched an attack to crash the  background check website. |