# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| After reviewing the incident backet analysis, it was discovered that the UDP protocol is unreachable due to traffic pressure on port 53 used to connect to the page request from the DNS Server.  After trying five times to reach the DNS server, it didn't work; it kept showing the following message, "undeliverable length \*\*\*", and that was because of too much traffic occurring on the 53 port.  The most likely issue for this situation is a DDOS attack on our system. Another reason is that we have a lot of customers, so we need a load balancer for our servers. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident occurred at **13:24:32.192571** when several customers reported they could not reach [**www.yummyrecipesforme.com**](http://www.yummyrecipesforme.com) and saw “destination port unreachable.” The network team ran **tcpdump** and found UDP DNS queries to **203.0.113.2:53** were met with ICMP replies **“udp port 53 unreachable,”** meaning the DNS host was reachable but not accepting UDP/53. The team began troubleshooting by checking the DNS service and server logs, verifying listeners on UDP/53, and reviewing firewall rules on **203.0.113.2**; they also prepared to contact the DNS administrator and switch clients to an alternate resolver as a temporary workaround. A likely cause is that the DNS daemon on **203.0.113.2** had stopped, crashed, or was misconfigured (so it wasn’t bound to UDP/53); less likely causes include a host firewall rejecting UDP/53 or a targeted attack affecting the DNS process. |