# 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: When the browser attempted to reach the DNS server to resolve the domain www.yummyrecipesforme.com, it used the UDP protocol on port 53.  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. This means the DNS server was not responding to UDP requests because the DNS service was either down or unreachable.  The port noted in the error message is used for:  **Port 53**, which is the default port used for DNS lookups via the **UDP protocol**.  The most likely issue is:  The DNS service on the server at IP 203.0.113.2 is not running or the firewall is blocking access to port 53, preventing the DNS resolution and causing users to be unable to access the website. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred:  1:24:32 PM, based on the tcpdump timestamps.  Explain how the IT team became aware of the incident:  Multiple customers reported they could not access the website and received a “destination port unreachable” error. The IT team attempted to visit the site and observed the same issue.  Explain the actions taken by the IT department to investigate the incident:  The team used tcpdump to analyze network traffic. They observed that the browser sent UDP DNS requests, which were followed by ICMP error messages stating "udp port 53 unreachable."  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):   DNS requests were sent to IP 203.0.113.2 on port 53.   ICMP replies showed the port was unreachable.   This suggests that either the DNS server was offline, misconfigured, or port 53 was being blocked.  Note a likely cause of the incident: The DNS server may be down or improperly configured, or there may be a firewall or network filter blocking port 53. This prevents domain name resolution, causing the website to be inaccessible. |