# 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 the DNS server is unreachable  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 DNS service  The most likely issue is the service down due to a successful DoS attack or the server has misconfigured. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred at 1:34pm, the IT team became aware of the incident when several customers contacted the company to report that they were unable to access the company website [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com/) and were getting a “destination error unreachable” error instead.  To investigate the incident security analysts in IT department attempted to visit the website but also received the error. They then used a packet analyzer tool to inspect the network traffic to and from the website in question.  Analysis of network traffic shows that the error is due to an unreachable DNS server. The network traffic log shows that whenever a request is made to DNS server 203.0.113.2 for the IP address of yummyrecipesforme.com, an ICMP echo message is received with the error message “port 53 unreachable” this means that this DNS server which is supposed to listening for DNS requests for yummyrecipesforme.com on the designated port 53 is actually not listening to request on that port.  It is likely that the DNS server in question is down due to a successful Denial of Service Attack or that the firewall has been misconfigured so that port 53 is not open for network requests, further action is needed to narrow down the root cause of this problem on the server. |