# 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.  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 length 254, 320, 150”  The port noted in the error message is used for: DNS protocol for TCP and UDP communications.  The most likely issue is: Port 53 is the standard DNS port. When it becomes unavailable it causes network issues such as not being able to resolve domain names i.e. google.com | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 1:24 PM  Explain how the IT team became aware of the incident:Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.  Explain the actions taken by the IT department to investigate the incident: I first attempted to reach the website myself and also received the reported error message “destination port unreachable.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): 192.51.100.15 > 203.0.113.2.domain. The IP address to the left of the greater than the source address, which is the computer’s IP address. The IP address to the right of the greater than the destination IP address. In this case, it is the IP address for the DNS server: 203.0.113.2.domain. For the ICMP error response, the source address is 203.0.113.2 and the destination is your computer's IP address 192.51.100.15. It was noted that no service was listening on the receiving DNS port. The plus sign after the query identification number indicates there are flags associated with the UDP message. The "A?" indicates a flag associated with the DNS request for an A record, where an A record maps a domain name to an IP address.  Note a likely cause of the incident: Port 53 may be restricted by the firewall. Ensure the port has been properly opened. |