# 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: UDP Port 53 is unreachable when customers attempted to load (or visit) website www.yummyrecipesforme.com  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: ICMP 203.0.113.2 UDP port 53 unreachable  The port noted in the error message is used for: UDP  The most likely issue is: Port 53 is unreachable when users try to access the website for yummyrecipesforme.com. Port 53 is used by the Domain Name System (DNS) which translates human-readable domain names into IP addresses so computers can communicate with one another seamlessly. The likely issue is the domain name is being mapped to the wrong domain name. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: The incident occurred in the afternoon.  Explain how the IT team became aware of the incident: Several customers of clients reported they couldn’t access the client company website.  Explain the actions taken by the IT department to investigate the incident: We loaded the website again while simultaneously using our network analyzer tool tcpdump.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):   * Destination port (UDP Port 53) unreachable * ICMP error * ICMP packers were sent 2 more times but resulted in same error * “+” sign indicates flags associated with UDP message * “A?” indicates flag associated with DNS request for A record   Note a likely cause of the incident:   * Domain Name was incorrectly mapped to the wrong domain name * The DNS request for IP address was unreachable b/c no service was listening to receiving DNS port |