# 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 there are no available ports in the DNS server.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: UDP port 53 is unreachable.  The port noted in the error message is used for: DNS queries, it is the standard port for DNS communication. This port is used to request the DNS to convert the domain name into the IP address for the website’s server.  The most likely issue is: the DNS server itself, it’s either down, misconfigured or the firewall or security group is blocking access to the port 53. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 13:24:36  Explain how the IT team became aware of the incident: Customers reported the incident stating that they’re not able to access the website www.yummyrecipesforme.com and received the error message ‘destination port unreachable’  Explain the actions taken by the IT department to investigate the incident: Using the network analyzer tool, tcpdump, to capture and analyse the packets attempting to access the website.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): any DNS queries to port 53 were unreachable and ICMP error messages were sent out saying ‘UDP port 53 unreachable’. This issue is regarding the DNS server at IP 203.0.113.2.  Note a likely cause of the incident: The DNS server is currently down, misconfigured or a firewall rule preventing access to the port 53. This may be the result of a DDoS or DoS attack which has prevented the access to the website www.yummyrecipesforme.com |