# 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 was attempting to reach the destination IP domain for yummyrecipesforme, but failed to connect.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: 203.0.113.2 udp port 53 unreachable length 254.  The port noted in the error message is used for: issues connecting to the DNS server. This is concluded from port 53 being associated with DNS protocol traffic.  The most likely issue is: the DNS server is not responding, which is further indicated by the flag in the first line of the log event, “35084+ A?”. The 35084 indicator is a UDP flag message and the associated “A?” symbol refers to flags with the DNS protocol operations. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 1:24 p.m.  Explain how the IT team became aware of the incident: Customers notified the organization when receiving the “destination port unreachable” message when attempting to visit the destination site.  Explain the actions taken by the IT department to investigate the incident: packet sniffing tests were utilized via tcpdump to create logs for the cyber professionals to analyze.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The packet sniffing test led to an analysis determining that the DNS port 53 was unreachable.  Note a likely cause of the incident: either the DNS server is down because of a Denial of Service attack or due to a misconfiguration blocked by a firewall protocol. |