# 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:   * DNS requests were made from a local machine to a DNS server, targeting port 53 for domain resolution.   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 (Domain Name System) services.   The most likely issue is:   * The DNS service on the server with IP 203.0.113.2 was either down or inaccessible, resulting in the ICMP error message. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred:   * 13:24:32.192571   Explain how the IT team became aware of the incident:   * While trying to access "yummyrecipesforme.com", an error message "destination port unreachable" appeared. This initiated the need for deeper analysis using tcpdump, a network analyzer tool.   Explain the actions taken by the IT department to investigate the incident:   * A packet capture was conducted using tcpdump to observe and analyze the network traffic between the local machine and the DNS server.   Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):   * The DNS request was made using UDP and targeted port 53 on the DNS server with IP address 203.0.113.2. * An ICMP error message was received in response to the DNS request, stating "udp port 53 unreachable", indicating no service was listening on that port. * Two subsequent DNS request attempts resulted in the same ICMP error message.   Note a likely cause of the incident:   * The DNS service on the target server (IP 203.0.113.2) was not operational or accessible at the time of the request, leading to the ICMP error message. The server could have been down, experiencing issues, or there could be firewall/security rules blocking the DNS request. |