# 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  An attempt was made to resolve the domain name yummyrecipesforme.com to its respective IP address.  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:  Domain Name System (DNS) queries and responses.  The most likely issue is:  The DNS server at IP 203.0.113.2 was not reachable on port 53, which is designated for DNS services, thereby hindering the DNS resolution process and preventing access to the website. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred:  The timestamps in the log show that the incident was first noticed at 13:24:32.192571.  Explain how the IT team became aware of the incident:  Several customers reported that they were unable to access the company website and were encountering the error "destination port unreachable". Additionally, upon visiting the website, the same error was encountered internally.  Explain the actions taken by the IT department to investigate the incident:   * Utilized the network analyzer tool, tcpdump, to capture and analyze network traffic while attempting to access the website. * Reviewed the DNS and ICMP traffic logs to identify the source of the error. * Noted the ICMP error messages indicating that the DNS server on port 53 was unreachable.   Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):   * The DNS request for resolving the domain name yummyrecipesforme.com to an IP address was sent using the UDP protocol. * The DNS server at IP address 203.0.113.2 was not reachable on port 53, as indicated by the ICMP error message "udp port 53 unreachable". * The issue persisted across multiple attempts to resolve the domain name, as indicated by repeated ICMP error messages.   Note a likely cause of the incident:  The most probable cause of the incident is a network or configuration issue on the DNS server at IP address 203.0.113.2, which prevented it from receiving or responding to DNS queries on port 53. This could be due to a network firewall rule, a misconfiguration on the DNS server, or the DNS service not being active or operational at the time of the incident. |