# 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 initiating device 192.51.100.15 is sending DNS queries to the server 203.0.113.2 on UDP port 53 but these queries are failing due to the server responding with ICMP “port unreachable” error messages.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:  “Port unreachable” this indicates that the requested port (UDP 53) is not accessible on the destination server.  The port noted in the error message is used for:  DNS (Domain Name System), which is responsible for resolving domain names yummyrecipesforme.com in IP address  The most likely issue is:  The DNS Server on the destination 203.0.113.2 is either   * No running or misconfigured. * Blocked by a Firewall or security policy preventing access to UDP port 53. * Overloaded or experiencing downtime. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred:  13:24:32 – Initial DNS query sent  13:24:36 – ICMP error “port unreachable” received.  13:26:32 – Second DNS query sent.  13:27:15 – ICMP error received.  13:28:32 – Third DNS query sent.  13:28:50 – ICMP error received.  This indicates multiple failed attempts over a span of approximately 4 minutes.  Explain how the IT team became aware of the incident:  The IT team likely noticed:   * Alerts generated by the monitoring system detecting ICMP error messages. * Application failures or delays in resolving domain names yummyrecipesforme.com. * End-user reports of issues with accessing internet resources.   Explain the actions taken by the IT department to investigate the incident:   * Received traffic logs: identified repeated DNS queries from 192.51.100.15 to 203.0.113.2. * Checked ICMP messages: found consistent “port unreachable” error for UDP port 53. * Examined DNS server configuration and availability: Looked for service outage, misconfigurations, or network firewall policies affecting UDP port 53. * Monitoring network activity: Confirmed whether the DNS queries were legitimate and if there was potential external interference.   Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):   * Port affected: UDP port 53 (used for DNS resolution) * Source device: IP 192.51.100.15 was attempting to query the domain yummyrecipesforme.com. * Destination server: IP 203.0.113.2 is either unavailable, misconfigured, or blocked by security settings. * Other observations: Repeated failed queries suggest the issue persisted for an extended period without resolution.   Note a likely cause of the incident:  The DNS server 203.0.113.2 is likely   * Offline or disabled: The DNS service may not be running. * Misconfigured: The server might not be listening on UDP port 53 or may have a restricted access policy. * Firewall issue: A network-level firewall or host-based security policy might be blocking traffic to UDP port 53. * Network outage: Routing issues or sever overloaded could prevent proper responses. |