# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The analysis of the DNS and ICMP traffic captured in the tcpdump log reveals a recurring issue with DNS resolution attempts made by the host at IP address 192.51.100.15. This host repeatedly attempts to resolve the domain name yummyrecipesforme.com by sending DNS queries to the server located at 203.0.113.2 using UDP port 53, which is the standard port for DNS queries. However, each of these requests is met with an ICMP error response from the server, specifically indicating that the destination port is unreachable.  This behavior shows that the UDP-based DNS queries are not being processed by the server, and instead, the server returns an ICMP "Port Unreachable" message. These ICMP messages confirm that port 53 on the DNS server is either closed or not listening for requests. UDP port 53 is universally used for DNS lookups, and when a response like "Port Unreachable" is received, it typically suggests that there is either no DNS service running on that port or the service is being actively blocked by a firewall or other network policy.  Based on this analysis, the most likely issue is that the DNS server at 203.0.113.2 is either misconfigured, not running a DNS service, or is deliberately blocking access to UDP port 53. As a result, DNS resolution for the requested domain cannot proceed, leading to repeated failures for any application or user depending on that domain name. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident began occurring at approximately 13:24:32 and continued with similar events logged at 13:26:32 and 13:28:32, as evidenced by the timestamps in the tcpdump output. Each event reflects an attempt by the internal host 192.51.100.15 to contact the external DNS server 203.0.113.2 to resolve a domain name, followed by an ICMP error indicating that UDP port 53 is unreachable.  The IT team became aware of the issue during routine network monitoring when they observed multiple ICMP responses indicating port errors. A closer inspection using tcpdump revealed that DNS resolution attempts were consistently failing and that each failure was tied to a returned ICMP error message from the DNS server. This prompted further investigation into whether the DNS server was operational and accessible from the client system.  To investigate the incident, the IT team analyzed the packet captures for both DNS queries and ICMP responses. It was quickly confirmed that all outbound DNS requests were targeting UDP port 53, and all inbound responses were ICMP "destination unreachable – port unreachable" messages. This confirmed that the DNS server was rejecting or ignoring requests on the expected service port. The IT department verified that the domain being queried (yummyrecipesforme.com) was valid but could not be resolved due to the server-side issue.  The key finding of the investigation is that the DNS server at 203.0.113.2 is not responding to DNS requests on UDP port 53. The likely cause of this is either a misconfiguration in the DNS server software, a firewall rule preventing access to port 53, or a failure in the DNS service itself on that server. As a result, client machines attempting to resolve domain names through this server are unable to do so, potentially disrupting application and internet access. |