# 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 UDP protocol reveals that DNS queries sent from the client to the DNS server are not being processed successfully. The DNS requests, which use UDP on port 53, are failing to reach their destination.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:  The ICMP error message returned is “udp port 53 unreachable.” This indicates that the DNS server is not accessible on UDP port 53, which is essential for DNS queries.  The port noted in the error message is used for:  The port noted in the error message, port 53, is used for the DNS (Domain Name System) service. DNS typically uses port 53 for both UDP (for standard queries) and TCP (for larger data transfers).  The most likely issue is:  The most likely issue is that the DNS server is either down, misconfigured, or there is a network-level issue (such as a firewall blocking traffic) preventing UDP traffic from reaching port 53. This is causing DNS resolution failures, which in turn prevents users from accessing the website. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred:  The incident occurred around 13:24:32 based on the timestamps in the `tcpdump` log, which show the first failed DNS request. The log indicates multiple subsequent failed attempts around 13:26:32 and 13:28:32, confirming ongoing issues.  Explain how the IT team became aware of the incident:  The IT team became aware of the incident after several customers reported being unable to access the client company website `www.yummyrecipesforme.com`. Users saw the error message "destination port unreachable" when trying to load the webpage. This prompted the IT team to investigate the reported connectivity issue.  Explain the actions taken by the IT department to investigate the incident: -   1. Replication of the Issue: The IT team attempted to access the website themselves and confirmed the error "destination port unreachable." 2. Network Traffic Analysis: The IT team used a network analyzer tool, `tcpdump`, to capture and analyze network traffic while attempting to load the webpage again. 3. Identification of the Error: By reviewing the `tcpdump` log, the IT team identified that DNS queries sent over the UDP protocol were not reaching the DNS server and were instead generating ICMP error messages indicating "udp port 53 unreachable."   Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): -   1. Affected Protocol and Port: The investigation revealed that UDP traffic on port 53(the standard port used for DNS services) was not being processed correctly. 2. DNS Server Issue: The DNS server at IP address 203.0.113.2 was not responding to DNS queries sent over UDP. Instead, it was returning ICMP error messages indicating that the port was unreachable. 3. ICMP Error Details: The ICMP error messages explicitly stated "udp port 53 unreachable," confirming that the DNS service on the server was not accessible for UDP requests.   Note a likely cause of the incident:  A likely cause of the incident is that the DNS server at IP address 203.0.113.2 was either down, misconfigured, or there was a network-level issue(such as a firewall or security setting) blocking or rejecting UDP traffic to port 53. This situation prevented the server from handling DNS queries, which are crucial for resolving domain names to IP addresses, thereby making the website inaccessible to users trying to connect. |