# 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 queries sent via UDP protocol to the DNS server at IP address 203.0.113.2 were undeliverable. * **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 service, which is responsible for resolving domain names to IP addresses. * **The most likely issue is:** The DNS server is not listening on port 53, which is preventing UDP packets from reaching it and resolving domain names, thereby causing the error. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| * **Time incident occurred:** The incident began at 13:24:32.192571 and was observed in repeated attempts at 13:26:32.192571 and 13:28:32.192571. * **Explain how the IT team became aware of the incident:** Customers reported being unable to access the website www.yummyrecipesforme.com, receiving the error message “Destination port unreachable.” The IT team confirmed the issue by attempting to access the website and receiving the same error. * **Explain the actions taken by the IT department to investigate the incident:**   + Attempted to access the website to replicate the reported issue.   + Loaded a network analyzer tool (tcpdump) to capture and analyze network traffic.   + Observed that outgoing UDP packets from the browser to the DNS server received ICMP error messages. * **Note key findings of the IT department’s investigation (i.e., details related to the port affected, DNS server, etc.):**   + UDP packets sent to DNS server (IP: 203.0.113.2) on port 53 failed.   + ICMP error messages indicated “udp port 53 unreachable,” confirming that the DNS server’s port 53 was not accepting requests.   + The error occurred repeatedly during multiple DNS queries at the following timestamps:     - 13:24:32.192571     - 13:26:32.192571     - 13:28:32.192571   + The source IP was 192.51.100.15, and the destination IP was 203.0.113.2.   + ICMP error packets provided additional details like varying lengths of 254, 320, and 150 bytes for each attempt. * **Note a likely cause of the incident:** The DNS server may have been misconfigured, its DNS service stopped, or port 53 could have been closed. This would prevent the server from processing DNS queries, resulting in the inability to resolve the domain name for the website. |