# 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 from the client to the DNS server at 203.0.113.2 are not being processed because the destination port is unreachable.  **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 services, specifically for handling domain name resolution queries over UDP.  **The most likely issue is:** The DNS server at 203.0.113.2 is either down, misconfigured, or not listening on UDP port 53—preventing domain name resolution for www.yummyrecipesforme.com and resulting in web access failure. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| **Time incident occurred:** The incident was first recorded at **13:24:32**, when the initial DNS request for www.yummyrecipesforme.com was sent and resulted in an ICMP error response indicating that **UDP port 53 was unreachable**.  **Explain how the IT team became aware of the incident:** Multiple customers reported that they were **unable to access the website** and received a **“destination port unreachable”**error message in their browsers. This prompted the IT team to investigate the issue using a network analyzer tool (tcpdump).  **Explain the actions taken by the IT department to investigate the incident:** The IT department attempted to load the website themselves while capturing network traffic using tcpdump. They inspected the outgoing DNS queries and the responses from the DNS server to determine where the failure occurred.  **Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):**   * The client system attempted to send **DNS queries over UDP** to the DNS server at 203.0.113.2, specifically to **UDP port 53**, which is the standard port used for DNS services. * Each DNS query resulted in an **ICMP error message**: udp port 53 unreachable. * This happened **consistently across three separate attempts** (at 13:24, 13:26, and 13:28). * No valid DNS response was received, meaning **DNS resolution failed** and the website could not be accessed.   **Note a likely cause of the incident:** The DNS server at 203.0.113.2 is **not accepting or processing UDP traffic on port 53**, possibly due to the **DNS service being down**, **misconfigured**, or **blocked by a firewall or ACL**. |