Cybersecurity Incident Report

Incident Report - Unreachable Port 53 for yummyrecipesforme.com

|  |
| --- |
| **Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log** |
| The incident involves the inability to access the client company website [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com), with users receiving a "destination port unreachable" error. Analysis of the DNS and ICMP traffic logs reveals that UDP packets sent to the DNS server (203.0.113.2) are met with ICMP packets containing the error message "udp port 53 unreachable." Port 53 is commonly associated with DNS services. The issue is repetitive, occurring at 13:24:32, 13:26:32, and 13:28:32. |
|

|  |
| --- |
| **Part 2: Explain your analysis of the data and provide at least one cause of the incident** |
| *Incident Details:* The incident was first reported by several customers who were unable to access [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com), prompting attention from the IT team. Further investigation using network analyzer tool tcpdump revealed that the DNS resolution process is encountering "udp port 53 unreachable" errors.  *Chronology of Events:*   * **13:24:32:** Initial DNS query for [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com), followed by ICMP error indicating UDP port 53 unreachable. * **13:26:32:** Repetition of DNS query and ICMP error. * **13:28:32:** Another occurrence of DNS query and ICMP error.   *Actions Taken:*   1. **Customer Reports Analysis:** Investigated customer reports to understand the issue's impact and nature. 2. **Initial Troubleshooting:** Checked server status, logs, and attempted to access the website from different locations. 3. **Network Traffic Analysis:** Utilized tcpdump to capture and analyze DNS-related traffic. 4. **Key Findings:** Identified repetitive "udp port 53 unreachable" errors in response to DNS queries.   *Possible Causes:*   1. **DNS Server Unavailability:** Suspected issues with the DNS server (203.0.113.2) may be causing the "udp port 53 unreachable" errors. 2. **Network Configuration:** Investigating potential network issues or misconfigurations affecting communication between source and destination.   *Next Steps:*   1. **Verify DNS Server Status:** Confirm availability and status of DNS server (203.0.113.2). 2. **Network Reachability Check:** Investigate network path for potential blockages or issues. 3. **DNS Configuration Review:** Ensure correct DNS configuration for [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com). 4. **Collaboration with DNS Provider:** If managed externally, collaborate with DNS provider to address issues. 5. **Communication with System Administrators:** Contact system administrators for the DNS server and web server to resolve the issue collaboratively.   *Possible Causes:*   1. **DNS Server Unavailability:** Suspected issues with the DNS server (203.0.113.2) may be causing the "udp port 53 unreachable" errors. |