Incident Report Summary – DNS Resolution Failure

Date/Time of Observation:

June 18, 2025 — 1:24 PM (timestamp `13:24:32.192571`)

Analyst:

Jason Phillips, Cybersecurity Analyst

Client:

Internal testing for `www.yummyrecipesforme.com`

Summary of the problem found in the DNS and ICMP traffic log.
The UDP protocol reveals that `www.yummyrecipesforme.com` is not loading properly. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message **"destination port unreachable" when attempting to establish a connection. Upon further inspection, a tcpdump (Network Analyzer Tool) was utilized and confirmed the error to be `"udp port 53 unreachable"` from the DNS server IP `203.0.113.2.`** The port noted in the error message is used for accepting/listening for query's between the DNS and IP, thus the error as it is unable to do so. The most likely issue upon initial analysis suggest the port is down, misconfigured, or perhaps a malicious attack on the server of some kind.

Analysis of the data and cause of the incident.

On June 18, 2025, at approximately 1:24 PM, multiple users reported that they were unable to access the website www.yummyrecipesforme.com and received the error message “destination port unreachable.” As a cybersecurity analyst, I attempted to reproduce the issue and encountered the same error. Using the network analysis tool tcpdump, I captured the DNS query traffic and identified that my computer was sending UDP packets to the DNS server at IP address 203.0.113.2 on port 53 in order to resolve the domain name. However, in response, the DNS server returned ICMP packets with the error message “udp port 53 unreachable.” This indicates that the DNS server was either down, misconfigured, or not accepting connections on the required port for DNS queries. Because DNS resolution failed, the browser could not obtain the IP address needed to establish an HTTPS connection to the website, resulting in the webpage being inaccessible. The core issue was determined to be a failure of the DNS service running on UDP port 53. This affected the UDP protocol specifically and caused DNS lookups to fail for the domain. It is recommended to verify that the DNS server is online, ensure that the DNS service is active and listening on port 53, and check for any firewall rules or network issues that might be blocking UDP traffic to this port. Additionally, configuring a backup DNS server could provide redundancy to prevent future disruptions.