Cybersecurity Incident Report

Incident: DNS resolution failure — www.yummyrecipesforme.com

Part 1: Provide a summary of the problem found in the tcpdump log

The tcpdump log captured at **13:24:32.192571** shows outbound DNS queries sent via **UDP** from the analyst's machine (**192.51.100.15**) to the DNS server (**203.0.113.2**) requesting an **A record** for www.yummyrecipesforme.com. Each request (identified by query ID 35084) was met with an **ICMP** response from the server stating udp port 53 unreachable. This request-and-response sequence repeated **three times** with identical failure messages. The affected protocols were **UDP** (used for DNS queries) and **ICMP** (used to return operational error status).

Part 2: Explain your analysis of the data and provide one solution to implement

Part 2: Explain your analysis of the data and provide one solution to implement
The issue was first reported when customers of the client company said they could not load www.yummyrecipesforme.com and received a "destination port unreachable" error. The analyst reproduced the issue and used tcpdump to capture traffic while attempting to load the page, also receiving the same failure message. The capture showed that the browser's DNS query (UDP, port 53) to the DNS server was answered with an ICMP "port unreachable" error message rather than a DNS response, meaning name resolution never completed. So, the browser never reached the HTTPS request stage.
Data Analysis: When users attempt to load www.yummyrecipesforme.com, the web browser must first resolve the domain name to an IP address via DNS before initiating an HTTPS connection. In this incident, DNS resolution failed because server 203.0.113.2 returned ICMP port unreachable errors for UDP port 53. Because the server actively responded with an ICMP error rather than timing out, basic IP routing to 203.0.113.2 was operational; however, the DNS daemon (service) on that server was either stopped, crashed, misconfigured, or blocked by local firewall rules. Without a successful DNS response, the browser could never learn the target IP address to send HTTPS requests, leaving customers unable to load the website. This points to a problem with the DNS service itself rather than a general network connectivity issue.
The issue has been escalated to the security engineering team for resolution.
Single Proposed Solution: Restart and verify the DNS service on server 203.0.113.2. Log into the DNS server, check the status of the DNS daemon (e.g., named, bind9, or system DNS service), restart the service if it has crashed, and verify using netstat or ss that the server is actively listening on UDP port 53. Additional next steps if the service is already running include reviewing firewall rules for port 53 and checking for recent configuration changes or signs of an attack (such as a denial-of-service attempt) that could have taken the service offline.
Suspected root cause: The DNS service on the target server is not running or not listening on port 53.