Network Protocol Analysis Report – DNS Port Unreachable

Objective

The goal of this exercise was to analyze tcpdump packet capture data to identify and interpret a 'destination port unreachable' error affecting the domain www.yummyrecipesforme.com. As a Cybersecurity Analyst, I was tasked with inspecting network traffic logs, identifying affected network protocols, and providing a root-cause assessment and solution.

Scenario Overview

A client reported that multiple users were unable to access the website www.yummyrecipesforme.com. When attempting to connect, users received the message: 'Destination port unreachable.' Upon investigation using tcpdump, I observed that the system attempted to query the Domain Name System (DNS) server to resolve the IP address for the website, but received ICMP responses indicating that UDP port 53 (the DNS service port) was unreachable. This pointed to a network-level communication issue between the client system and the DNS service.

Tools & Methodology

- Tools Used: tcpdump, Browser (HTTP/HTTPS requests)
- Protocols Analyzed: UDP, ICMP, DNS
- Key Ports: Port 53 (DNS), Port 443 (HTTPS)
- Method: Captured live packet data while attempting to load the website and examined timestamps, protocol behavior, and error responses.

Step 1 – Summary of tcpdump Log Analysis

Log Findings:

```
13:24:32.192571 IP 192.51.100.15.35084 > 203.0.113.2.domain: 35084+ A?
www.yummyrecipesforme.com.
13:24:32.192878 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable
```

Analysis Summary:

• The first packet shows an outbound UDP request from the local workstation (192.51.100.15) to the DNS server (203.0.113.2) on port 53 requesting resolution of the domain name. • The subsequent ICMP message indicates that the DNS service on port 53 is unreachable. • Repeated ICMP error messages confirmed continued delivery failures. • The affected protocol in this case is UDP, specifically traffic related to DNS resolution.

Interpretation: The DNS query packets were unable to reach their intended destination because port 53 on the DNS server was not accepting traffic. This prevented domain name resolution and led to the 'destination port unreachable' message when users attempted to access the website.

Step 2 – Incident Analysis and Resolution Plan

Category	**Details**
Time Detected	1:24 p.m.
Event Description	Multiple client users unable to access www.yummyrecipesforme.com ; browser displayed “destination port unreachable.”
Observed Behavior	UDP requests to the DNS server failed; ICMP returned 'udp port 53 unreachable.'
Protocols Affected	UDP (DNS), ICMP
Error Type	ICMP Type 3 (Destination Unreachable), Code 3 (Port Unreachable)
Root Cause (Suspected)	The DNS service on the client’s configured DNS server (203.0.113.2) was either down, misconfigured, or blocked by a firewall.
Impact	Users unable to resolve domain names → website inaccessible.
Status	Reported to Security Engineers for remediation.

Technical Analysis Summary

1. Issue Detection: The ICMP 'port unreachable' message clearly indicated a lower-layer network issue with DNS communication.
2. Protocol Chain: Browser initiated a DNS lookup via UDP on port 53. The DNS server responded with an ICMP Type 3 message ('port unreachable'). Without DNS resolution, browsers could not complete the HTTPS connection.
3. Pattern Observed: The repeated ICMP responses showed persistence of the outage. No other network protocols (TCP/HTTP) were initiated due to DNS failure.

Solution & Next Steps

Proposed Resolution Steps:

1. Verify that the DNS service on port 53 is operational on the DNS server (203.0.113.2). 2. Check firewall and access control lists (ACLs) to ensure that UDP port 53 traffic is allowed between client and DNS server.

3. Confirm that the DNS server is properly configured and not blocking requests from the client subnet.

4. Test name resolution using an alternate DNS server (e.g., 8.8.8.8).
5. After confirming service restoration, retest access to www.yummyrecipesforme.com using tcpdump or dig/nslookup.

Expected Outcome: Once DNS connectivity on UDP port 53 is restored, users will again be able to resolve the domain and access the website normally via HTTPS.

Conclusion

The tcpdump analysis confirmed that the UDP protocol on port 53—used by the DNS service—was affected during this incident. The ICMP 'destination port unreachable' message indicated that the DNS server was not accepting requests, which prevented domain resolution and blocked web access. By identifying the root cause and escalation path, this investigation demonstrated effective network-level troubleshooting, packet analysis, and incident documentation aligned with professional SOC reporting standards.

Cybersecurity Relevance

This investigation strengthened practical experience in: packet analysis with tcpdump, identifying impacted network layers and services, interpreting ICMP error codes, and communicating findings via structured incident reports. These skills directly support SOC operations, incident response, and network defense roles.