LOW-IMPACT TCP SYN SCAN & TRAFFIC VALIDATION (CLI-BASED)

December 23, 2025

1. Overview

This project documents a controlled analysis of local network traffic using **command-line tools only**. The main focus to verify whether specific TCP activity observed on a home router represented normal traffic or intentional probing, while keeping the impact on the network as low as possible.

Rather than relying on alerts or visual spikes, the analysis was done at the **packet behavior level**, with emphasis on TCP flags, timing, and response patterns.

2. Objectives

- Perform a **minimal and non-disruptive TCP SYN scan**
- Distinguish **normal client traffic** from **probing behavior**
- Validate findings using **raw packet captures**
- Avoid assumptions based solely on traffic volume

3. Environment

- Network: Local LAN (192.168.1.0/24)
- Target device: Router (192.168.1.1)
- Analysis host: 192.168.1.12
- Interface: Wi-Fi (wlp3s0)
- Scope: Short, event-based observation

4. Tools Used (CLI Only)

- **nmap** – Targeted TCP SYN scanning
- **tcpdump** – Raw packet inspection and TCP flag analysis

- **tshark** – Interval-based traffic statistics

No GUI packet analyzers or pre-built monitoring platforms were used.

5. Methodology

Targeted SYN Scanning

A small set of common service ports (22, 80, 443) was scanned using a **low-and-slow approach**:

- Long scan delays
- Minimal retries
- No aggressive service detection

This was done to confirm port states without generating noticeable traffic bursts.

Packet-Level Validation

During scanning, packets were captured in real time to observe:

- TCP flag sequences
- Session establishment behavior
- Client-side resets

Traffic Stability Check

Traffic statistics were reviewed to ensure that the scan did not create abnormal spikes or sustained load on the network.

6. Observations

- Port 80 responded with SYN-ACK followed by client RST
- Ports 22 and 443 returned immediate RST responses
- No full TCP sessions were established
- Traffic volume remained stable and low

7. Analysis

The observed SYN → SYN-ACK → RST pattern confirms intentional probing behavior without service interaction.
Response consistency and low RTT indicate a stable embedded network device.

8. Conclusion

The analysis confirms that low-impact TCP scanning can be safely validated through packet inspection.
This approach avoids unnecessary noise while maintaining technical accuracy.

9. Lessons Learned

- Traffic volume alone is not a reliable indicator of scanning activity
- TCP flag sequences provide more accurate insight than port states alone
- A SYN scan can remain almost invisible when timing and retries are controlled
- Packet-level validation prevents false assumptions based on tool output
- Not every scan requires aggressive options like `-A` or service detection
- Understanding *when to stop* is as important as knowing *how to scan*

Prepared by:
Falah Rohmatuloh | Karedok
Network & Security Analysis (CLI)
Date: December 2025