

Forum:[Hack Forums](#)

Thread: [I Built My Own Recon Pipeline Instead of Using 15 Different Tools](#)

zyco1 - October 19, 2026, 2:03 am

I've been experimenting with building a lightweight reconnaissance pipeline that combines subdomain discovery, DNS resolution, HTTP probing, and technology fingerprinting into one workflow. Tools like Subfinder, dnsx, httpx, and WhatWeb each handle a different part of the process, but managing their separate outputs can get messy when you're working with multiple authorized targets. My current focus is on building a consistent output format, removing duplicate results, tracking changes between scans, and generating a readable summary at the end.

One feature I'd really like to implement is historical comparison, where the pipeline highlights newly discovered subdomains, changed HTTP status codes, and services that have become reachable since the previous scan. I'm also considering a small SQLite database so I can store results without having to maintain a full database server. The challenge is deciding which parts deserve automation and which parts should remain manual.

For people who have built their own recon frameworks, did you start with a shell script, Python, or Go? How do you handle errors and inconsistent tool output without making the code unnecessarily complicated? I'd be interested in hearing about your architecture, especially if you've found a way to make the results genuinely more useful than running each tool individually.