🔥 Great, you’re now moving into **WSTG-INFO-09: Test for Subdomain Takeover** — this is a **very real-world vulnerability** often missed by orgs. Let’s break it down step by step with your listed tools.

**🛠 Test for Subdomain Takeover**

**🎯 Goal**

Identify subdomains that **point to an external service (CNAME record)** but are **not claimed/configured**, e.g.:

shop.example.com → CNAME → myshopify.com

If the myshopify.com account doesn’t exist, an attacker can register it and **take over shop.example.com**.

**1. Discovery of Subdomains**

**a) dnsrecon**

dnsrecon -d example.com -t brt

Brute-force subdomains and get DNS records (esp. CNAME).

**b) nslookup**

Quick check for CNAMEs:

nslookup shop.example.com

If it resolves to a 3rd-party service → candidate for takeover.

**c) sublister**

sublist3r -d example.com

Enumerates subdomains using search engines, useful for finding abandoned ones.

**d) dnsdumpster**

Web-based tool ([https://dnsdumpster.com](https://dnsdumpster.com/)) → gives **visual DNS mapping** with CNAMEs.

**e) subdomainfinder**

Similar to Sublist3r, automates discovery:

subfinder -d example.com

**f) spyse.com**

Now part of **SecurityTrails/Spyse APIs** → rich subdomain database for enumeration.

**2. Identify Takeover Candidates**

* Look for **CNAME records** pointing to:
  + GitHub Pages (.github.io)
  + AWS S3 buckets
  + Azure/Heroku apps
  + Shopify, WordPress, etc.
* If request returns **NXDOMAIN** or **“No such host”** → possible takeover.

Example:

dig shop.example.com

Output:

shop.example.com. CNAME myshopify.com.

But visiting it → “Site not found” → vulnerable.

**3. Exploitation Scenario (theory only ✅)**

1. Attacker registers the unclaimed 3rd-party service (e.g., creates a Shopify site with that subdomain).
2. The subdomain (shop.example.com) now resolves to attacker-controlled content.
3. Used for **phishing**, **XSS injection**, or **data exfiltration**.

**4. Defenses**

* Monitor DNS records regularly.
* Remove stale CNAMEs pointing to decommissioned services.
* Use automated scanners (SecurityTrails, Detectify, Aquatone).
* Implement **DNS monitoring alerts** for NXDOMAIN or dangling records.

✅ **Summary**

* Tools: dnsrecon, nslookup, sublister, dnsdumpster, subdomainfinder, spyse.com.
* Look for **CNAME → external service → not configured**.
* High risk: attacker can fully **control a subdomain** of the target org.

👉 Do you want me to create a **step-by-step challenge lab** (where you simulate a dangling CNAME on your own domain and practice the takeover) or just keep it as **theoretical guidance**?