**🕵️ Spyse (Spyse/SecurityTrails) – OSINT for Infrastructure Recon**

**Level:** Beginner

**Category:** OSINT / Reconnaissance / Asset Discovery

**🧠 What is Spyse?**

**Spyse** was a **search engine for internet assets**, letting you find **all public data** about:

* Domains
* IP addresses
* Subdomains
* Open ports
* SSL certificates
* DNS records
* Technologies used by websites

Spyse helped map out **entire infrastructures of companies or targets** using just a domain or IP.

📝 **Update:** Spyse data is now merged into tools like:

* 🌐 [https://securitytrails.com](https://securitytrails.com/)
* CLI tools like spyse.py (still works if set up)

**🔍 Why Use Spyse?**

| **Purpose** | **Benefit** |
| --- | --- |
| 🧠 Passive Recon | No alerts to the target, fully stealth |
| 🏗️ Map Infrastructure | See related IPs, subdomains, DNS records |
| 🔒 Discover Weaknesses | Find old, exposed services or forgotten subdomains |
| 🔎 Correlate Entities | Find what other domains/IPs are linked to the same company or email |

**🧪 Typical Use Cases (as a beginner)**

**✅ 1. Discover Subdomains**

Target: tesla.com

Spyse/SecurityTrails may show:

- api.tesla.com

- auth.tesla.com

- dev.tesla.com

- staging.tesla.com

🔎 These subdomains are often forgotten and vulnerable (great for bug bounties!).

**✅ 2. Discover Open Ports & Services**

Search by IP to find open ports like:

IP: 104.18.2.12

Ports: 80 (HTTP), 443 (HTTPS), 21 (FTP), 22 (SSH)

You can also see:

* Banner info
* SSL certificates
* HTTP headers

**✅ 3. DNS Records**

Get:

* A records (IP)
* MX (mail servers)
* TXT (SPF, DKIM)
* NS (name servers)

🔐 **Bonus**: Misconfigured TXT records might reveal internal info.

**✅ 4. Track Ownership or Fingerprints**

If you know:

* A company name
* ASN
* SSL Cert

Spyse can map **all domains or IPs owned by that company** — even if they use different registrars.

**🧰 How to Use Spyse-like Functionality Today**

Since **Spyse’s UI is no longer public**, use:

**🔹 Option 1: SecurityTrails (Most Similar)**

* Website: [https://securitytrails.com](https://securitytrails.com/)
* Free for basic recon
* Just enter a domain → see DNS, subdomains, IPs, ASNs, tech stack, etc.

**🔹 Option 2: Spyse CLI Tool (if available)**

Some versions of the CLI tool still work:

git clone https://github.com/SpyseHQ/spyse-python.git

cd spyse-python

pip install -r requirements.txt

* Set API key (if you have one)
* Run:

python3 spyse.py -d example.com

**🛡️ Sample OSINT Flow with Spyse-like Tools**

| **Step** | **Tool** | **What You Discover** |
| --- | --- | --- |
| 1. Start with Domain | Spyse/SecurityTrails | Subdomains, DNS, IPs |
| 2. Check IPs | Spyse/SecurityTrails | Open ports, services |
| 3. Check ASN | Spyse/SecurityTrails | Infrastructure of entire company |
| 4. Cross-check | Shodan, SpiderFoot | Vulnerabilities, screenshots |
| 5. Correlate | Maltego/Amass | Visual links between data |

**⚠️ Legal Note**

❗ Use only for **educational**, **ethical hacking**, or **bug bounty** purposes.  
Passive recon is stealthy — but **using results to hack targets is illegal** without permission.

**✅ Summary**

| **Feature** | **What It Does** |
| --- | --- |
| Domain Recon | Find DNS records, IPs, subdomains |
| Infra Mapping | Discover hidden parts of companies’ networks |
| IP Search | View ports, services, SSL certs |
| Passive OSINT | Safe for ethical hacking & red teaming |