🕷️ SpiderFoot Ultimate Cheat Sheet

Category: OSINT / Reconnaissance
Mode: GUI (Web-based) & CLI

🔷 1. Introduction

- **SpiderFoot** = OSINT automation tool for reconnaissance.
- Collects data from **100+ data sources** (whois, DNS, leaks, social media, Shodan, etc.).
- Can run via **GUI (browser interface)** or **CLI (scripted scans)**.
- Useful for: Penetration testers, Red Teams, Threat Intelligence, Bug Bounty.

🔷 2. Installation & Setup

Kali Linux / Linux

```
git clone https://github.com/smicallef/spiderfoot.git
cd spiderfoot
pip3 install -r requirements.txt
python3 ./sf.py -l 127.0.0.1:5001
```

Run GUI

```
python3 ./sf.py -l 127.0.0.1:5001
```

Open browser → http://127.0.0.1:5001

Run CLI

```
python3 ./sfcli.py --help
```

🔷 3. Basic Usage (Beginner)

Start Web UI

python3 ./sf.py -l 127.0.0.1:5001

Quick Scan (Domain Example)

python3 ./sfcli.py -s example.com -m all

- -s = target (IP, domain, email, ASN, name)
- -m all = run all modules

Limit to Specific Modules

python3 ./sfcli.py -s example.com -m sfp_dnsresolve,sfp_shodan

Save Output

python3 ./sfcli.py -s example.com -m all -o spiderfoot_results.json

---

🔷 4. Intermediate Usage

Target Types Supported

- Domain → example.com
- IP → 192.168.1.1
- Email → admin@example.com
- Username → john_doe
- ASN → AS12345
- Subnet → 192.168.1.0/24

Common Options

--help # Show help

-s TARGET # Set target (domain, IP, email, etc.)

-m MODULES # Specify modules (comma separated)

-o FORMAT # Output format (json, csv, sqlite, gexf)

-f TYPE # Filter output (IP, domain, email, etc.)

Run All Available Modules

python3 ./sfcli.py -s example.com -m all -o csv

Run With Data Source API Keys (Advanced)

Add API keys in → spiderfoot/config/ or Web UI → Settings → API Keys.

🔷 5. Advanced Usage (Pro Level)

1. Silent CLI Scan with JSON Output

python3 ./sfcli.py -s example.com -m all -o json > results.json

2. Export Graph for Maltego / Visualization

python3 ./sfcli.py -s example.com -m all -o gexf > results.gexf

3. Focused Investigation (Emails only)

python3 ./sfcli.py -s example.com -m sfp_email

4. Use with Shodan

python3 ./sfcli.py -s example.com -m sfp_shodan

5. Use with HaveIBeenPwned (HIBP)

python3 ./sfcli.py -s admin@example.com -m sfp_haveibeenpwned

6. Use with VirusTotal

python3 ./sfcli.py -s example.com -m sfp_virustotal

🔷 6. Modules Categories

Category	Example Modules
DNS/WHOIS	sfp_dnsresolve, sfp_whois, sfp_bing
OSINT	sfp_shodan, sfp_virustotal, sfp_github
Leaks	sfp_haveibeenpwned, sfp_breach
Infra	sfp_asn, sfp_subdomain, sfp_whatcms
Social Media	sfp_twitter, sfp_facebook, sfp_linkedin

Category	Example Modules
Dark Web	sfp_onion, sfp_darksearch

🔷 7. Output Formats

Format	Usage
json	API integration, automation
csv	Spreadsheet reports
sqlite	Database queries
gexf	Import into Gephi/Maltego for visualization

🔷 8. Pro Tips & Notes

✅ Always add API keys in settings for best results (Shodan, HIBP, VirusTotal).
✅ Run **focused scans** instead of all modules to avoid noisy results.
✅ Use **filters** (-f) for faster analysis.
✅ For professional reports → export in **CSV + GEXF** for visualization.
✅ Combine SpiderFoot results with **Recon-ng, Maltego, or Nmap** for deeper penetration testing.