SpiderFoot — Professional Cheat Sheet

Compact, actionable OSINT automation reference

Overview

SpiderFoot is an open-source OSINT reconnaissance tool that automates the discovery of information about domains, IP addresses, hostnames, ASNs, emails and people. It supports both a web UI and CLI and integrates with many external APIs (Shodan, HaveIBeenPwned, VirusTotal, etc.) for richer results.

Installation

Commands:

Clone & enter repo	git clone https://github.com/smicallef/spiderfoot.git && cd spide
Install deps	pip3 install -r requirements.txt
Run help	python3 sf.py -h

Running SpiderFoot

Web Interface

```
Start web UI (default local):
python3 sf.py -l 127.0.0.1:5001
```

Open browser: http://127.0.0.1:5001

CLI mode

```
Common pattern:
python3 sf.py -s -m -o -f -t
```

Target Types (examples)

Domain	example.com
IP address	192.0.2.1
Hostname	mail.example.com
Subnet	203.0.113.0/24
ASN	AS15169
Email / Person	john@example.com

Common CLI Options

-s <target>	Specify the target (domain, IP, ASN, email, etc.)
-m <modules>	Run specific modules (comma-separated)
-M	List all available modules
-o <format>	Output format: csv, json, sqlite, gexf
-f	Use only relevant modules for this target (faster)
-t <threads>	Number of threads to use
-L	List all supported data types

Command Examples

Full scan (CSV, relevant modules, 10 threads)	python3 sf.py -s example.com -o csv -f -t 10

Specific modules, JSON output	python3 sf.py -s example.com -m sfp_dnsresolve,sfp_sslcert -o jso
Save to local DB (SQLite)	python3 sf.py -s example.com -o sqlite
List modules	python3 sf.py -M
List supported data types	python3 sf.py -L

Key Modules (select examples)

sfp_dnsresolve	Resolve DNS names, gather A/AAAA records
sfp_subdomains	Discover subdomains via bruteforce/search engines
sfp_sslcert	Extract SSL certificate details & SANs
sfp_arin	WHOIS / ASN lookups
sfp_email	Discover email addresses
sfp_accounts	Search usernames across platforms
sfp_webmeta	Harvest web page metadata
sfp_vuln	Search known vulnerabilities
sfp_shodan	Shodan integration (requires API key)

Output Formats & Use Cases

csv	Quick import to spreadsheets
json	Automation, parsing by scripts/APIs
sqlite	Store results for later re-analysis
gexf	Graph export (Gephi / Maltego)

Professional Tips & Best Practices

- Use -f to limit modules to those relevant to your target and speed up scans.
- Store results in sqlite when you want to query/export later.
- Integrate API keys (Shodan, VirusTotal, HaveIBeenPwned) in spiderfoot.conf for richer data.
- Export GEXF for graph analysis in Gephi or for Maltego transforms.
- When operational security matters, run a reduced set of modules and throttle threads.
- Combine SpiderFoot with additional tooling (Nmap, Amass, Subfinder) to enrich findings.

Notes

Always respect the law and the terms of service of services you query. Only run SpiderFoot against targets you are authorized to test. For advanced usage, edit spiderfoot.conf to enable API keys and tweak module settings. Review module-specific rate limits before large scans.