SpiderFoot Cheat Sheet

What is SpiderFoot?

SpiderFoot is an **automated OSINT (Open-Source Intelligence) tool** that helps gather information on targets from **over 200 data sources**. It is useful for **security assessments, threat intelligence, and reconnaissance**.

Key Features of SpiderFoot

✅ **Automated Data Collection** – Runs queries on multiple sources automatically. ✅ **Data Correlation** – Links different data points to identify relationships. ✅ **Customization** – Choose which modules to use for specific investigations. ✅ **Web-Based Interface & CLI Support** – Run scans via GUI or command line. ✅ **API Support** – Use APIs for third-party integrations. ✅ **Report Generation** – Export findings in various formats (CSV, JSON, HTML, etc.).

Installing SpiderFoot

Linux/macOS:

```
# Install dependencies
sudo apt install python3-pip

# Clone the repository
git clone https://github.com/smicallef/spiderfoot.git
cd spiderfoot

# Install required Python packages
pip3 install -r requirements.txt

# Run SpiderFoot
python3 sf.py -l 127.0.0.1:5001
```

Windows:

1. Install Python (3.x).
2. Download SpiderFoot from GitHub.
3. Install dependencies using `pip install -r requirements.txt`.
4. Run `python sf.py -l 127.0.0.1:5001`.
5. Open `http://127.0.0.1:5001` in a browser.

Running a Scan (GUI)

1. Open the **SpiderFoot web interface** (`http://127.0.0.1:5001`).
2. Click **New Scan**.

3. Enter a target (e.g., domain, IP, email, username, etc.).
4. Choose the **modules** to use (or select all for full scan).
5. Click **Start Scan** and wait for results.

Running a Scan (CLI)

```
python3 sf.py -m all -s target.com
```

Options:

- `-m all` → Enable all modules.
- `-s target.com` → Specify the target.
- `-o output.html` → Save results in an HTML file.

Important Modules & Use Cases

Module	Purpose
`sfp_dns`	Finds DNS records, subdomains, and MX records.
`sfp_social`	Checks for social media accounts linked to an identity.
`sfp_pwned`	Checks for compromised accounts in data breaches.
`sfp_shodan`	Searches for exposed devices and services using Shodan.
`sfp_googlesearch`	Uses Google Dorking to find indexed data.
`sfp_bgpview`	Retrieves IP information and network details.
`sfp_darkweb`	Looks for references to the target in dark web sources.
`sfp_email`	Finds associated email addresses and leaks.

Analyzing the Results

- **Red Flags** 🚩 – Exposed credentials, leaked emails, misconfigured servers.
- **Patterns & Connections** 🔗 – Identify relationships between data points.
- **Export Data** 📁 – Save findings for further analysis.

Best Practices

✅ Use **specific modules** to avoid unnecessary noise.

✅ Cross-check results with other OSINT tools (e.g., Maltego, Shodan).

✅ Be **ethical** – Do not target individuals or unauthorized entities.

✅ Regularly **update** SpiderFoot for the latest features and fixes.

SpiderFoot is a powerful OSINT automation tool that saves time and provides deep insights into a target's **digital footprint**. However, always **use it responsibly** and ensure you have permission to scan a target. Happy hunting! 🔍