

TheHarvester Cheatsheet

TheHarvester is an Open Source Intelligence (OSINT) tool used to gather publicly available information about a domain. It helps in collecting emails, subdomains, IPs, and more from various sources.

Basic Syntax

```
TheHarvester -d <domain> -b <source> [options]
```

- `-d` → Specifies the target domain (e.g., `tesla.com`)
- `-b` → Specifies the data source (e.g., `google`, `bing`, `all`)

Common Usage

1. Basic OSINT on a Domain

```
theHarvester -d tesla.com -b google
```

(Finds publicly available emails & subdomains using Google.)

2. Full Recon on a Domain

```
theHarvester -d tesla.com -b all -l 200 -f tesla_report.txt
```

*(Finds **all** data, limits to 200 results, and saves to `tesla_report.txt`.)*

3. Shodan Lookup (Exposed Devices)

```
theHarvester -d tesla.com -b shodan
```

*(Finds **internet-exposed devices** related to Tesla.)*

4. Save Results to a File

```
theHarvester -d tesla.com -b google -f results.txt
```

(Saves results to `results.txt`.)

5. Verbose Mode (More Details)

```
theHarvester -d tesla.com -b all -v
```

(Enables verbose mode for more detailed output.)

Available Data Sources (`-b` Parameter)

Instead of `all`, you can specify a particular source:





| Source | Description |
|--------|---|
| google | Searches Google for emails and subdomains |

| | |
|-------------|--|
| bing | Uses Bing for information gathering |
| crtsh | SSL certificate transparency logs |
| dnsdumpster | Finds subdomains & DNS records |
| linkedin | Collects employee names (if public) |
| shodan | Finds exposed devices (requires API key) |
| baidu | Uses Baidu search engine |
| exalead | Uses Exalead search engine |

Advanced Options

| Option | Description | Example |
|-----------|---|---------------|
| -l <num> | Limits number of results (default: 500) | -l 100 |
| -f <file> | Saves output to a file | -f output.txt |
| -v | Enables verbose mode | -v |
| -h | Displays help menu | -h |
| -n | No banner (clean output) | -n |

Pro Tips

 Use `-b all` to get a **comprehensive report**.
  Use `-l 100` to **avoid getting rate-limited** by sources.
  Always have **permission** before scanning a domain.
  Combine with **Shodan API** for deeper insights.

Ethical Reminder

- **Only scan domains you have permission to investigate.**
- **Misuse of TheHarvester can be illegal.**
- **Use OSINT responsibly for security research.**