**🕵️‍♂️ TheHarvester Ultimate Cheat Sheet**

**Information Gathering & OSINT Tool**

**🔹 Basic Syntax**

| **Command** | **Description** |
| --- | --- |
| theharvester -d <domain> -b <source> | Run search against a single source |
| theharvester -d <domain> -l <limit> -b <source> | Limit number of results per source |
| theharvester -d <domain> -b all | Search using all available sources |
| theharvester -h | Display help menu |

**🔹 Common Options**

| **Option** | **Description** |
| --- | --- |
| -d <domain> | Target domain (e.g., example.com) |
| -b <source> | Data source (e.g., google, bing, baidu, linkedin) |
| -l <limit> | Limit number of results |
| -s <start> | Starting result number |
| -f <file.html> | Save results to an HTML/XML file |
| -v | Verbose mode (detailed output) |
| -h | Show help menu |

**🔹 Popular Data Sources**

| **Source** | **Use** |
| --- | --- |
| google | Emails, subdomains |
| bing | Emails, subdomains |
| baidu | Asian sources |
| linkedin | Employee names & info |
| crtsh | Certificate transparency logs |
| hunter | Email harvesting (API required) |
| duckduckgo | Alternative search engine |
| all | Use all sources |

**🔹 Examples**

| **Command** | **Purpose** |
| --- | --- |
| theharvester -d example.com -b google | Gather emails & hosts from Google |
| theharvester -d example.com -b bing -l 200 | Get 200 results from Bing |
| theharvester -d example.com -b linkedin | Extract employee info from LinkedIn |
| theharvester -d example.com -b crtsh | Find subdomains from SSL certificates |
| theharvester -d example.com -b all -f results.html | Run on all sources, save to HTML |

**🔹 Output Formats**

| **Option** | **Description** |
| --- | --- |
| -f report.html | Save results in HTML |
| -f report.xml | Save results in XML |
| Default | Prints to terminal |

**🔹 Tips & Notes**

* Use multiple sources (-b all) for broader coverage.
* Limit queries (-l) to avoid API rate limiting.
* Save reports (-f) for later analysis or sharing with your team.
* Combine with **Maltego, Recon-ng, or SpiderFoot** for advanced OSINT.
* Use **crtsh + google + bing** combo for maximum subdomain coverage.