**1. Google Hacking Database (GHDB)**

* **Purpose**: Uses specially crafted search queries, also known as "Google Dorks," to find sensitive information exposed online.
* **How to Use**: Search by combining keywords with Google operators (e.g., site:example.com intitle:"index of").
* **Effectiveness**: **Highly effective** for identifying sensitive data exposed on the web, such as login portals, configuration files, and directories.

**2. Creepy Dorks**

* **Purpose**: Gathers geolocation information based on public social media posts, allowing attackers to map a target’s physical movements.
* **How to Use**: Input a username or other identifying information into Creepy to obtain geolocation data.
* **Effectiveness**: **Useful** for physical security reconnaissance or tracking social media activity.

**3. Sublist3r**

* **Purpose**: Subdomain enumeration tool that helps gather information on subdomains of a target.
* **How to Use**: Run sublist3r -d example.com to enumerate subdomains.
* **Effectiveness**: **Highly effective** for finding subdomains, particularly useful for mapping an organization's external assets.

**4. Amass**

* **Purpose**: Advanced asset discovery tool focused on subdomain enumeration, DNS information, and network mapping.
* **How to Use**: Run amass enum -d example.com for subdomain discovery.
* **Effectiveness**: **Extremely effective** for large-scale and automated reconnaissance, particularly for discovering external assets.

**5. Subfinder**

* **Purpose**: Fast subdomain enumeration tool for identifying subdomains from multiple sources.
* **How to Use**: Run subfinder -d example.com to list subdomains.
* **Effectiveness**: **Highly effective** and fast for enumerating subdomains. It's known for its speed and accuracy.

**6. waybackurl**

* **Purpose**: Retrieves archived URLs of a target from the Wayback Machine, which is useful for discovering previously available content or endpoints.
* **How to Use**: Run echo example.com | waybackurls to gather historical URLs.
* **Effectiveness**: **Very useful** for discovering deprecated or removed pages and endpoints that could still be exploitable.

**7. katana**

* **Purpose**: A fast, self-contained web crawler designed to extract URLs, endpoints, and other information from web applications.
* **How to Use**: Run katana -u example.com to scan and retrieve URLs.
* **Effectiveness**: **Highly effective** for web asset discovery and provides results quickly.