A Practical Guide to Subdominator

Eyad Islam El-Taher

November 21, 2025

1 Introduction

Subdominator is a powerful tool for passive subdomain enumeration during bug hunting and reconnaissance processes. It is designed to help researchers and cybersecurity professionals discover potential security vulnerabilities by efficiently enumerating subdomains using various free passive resources.

2 Features

- **Fast and Powerful:** Efficiently enumerates subdomains with optimized performance
- **Extensive Coverage:** 50+ passive resources for comprehensive subdomain discovery
- **Configurable API Keys:** Flexible setup for various data sources
- **Integrated Notification System:** Alerts via Slack, Pushbullet, etc.
- **Local Database Support:** Store and manage enumeration data locally
- **Multiple Output Formats:** Support for TXT, HTML, PDF, and JSON formats
- **Interactive Shell Mode:** Work with subdominator database and generate reports

3 Installation

3.1 Prerequisites

Ensure you have Python 3.12 or later installed:

```
python3 --version
```

3.2 Installation Methods

3.2.1 Install from PyPI (Recommended)

```
pip install --upgrade subdominator
```

3.2.2 Install from GitHub

```
pip install --upgrade git+https://github.com/RevoltSecurities/
    Subdominator
```

3.2.3 Install using PIPX

```
pipx install subdominator
```

3.2.4 Install from Source

```
git clone https://github.com/RevoltSecurities/Subdominator.git
cd Subdominator
pip install --upgrade pip
pip install -r requirements.txt
```

3.3 Verification

Verify installation by running:

```
subdominator --help
```

4 Configuration

4.1 YAML Configuration Updates

Existing users need to update their config YAML file with new resources. Open the config file at:

```
$HOME/.config/Subdominator/provider-config.yaml
```

Add the following resources:

```
builwith:
  - your-api-key1
  - your-api-key2

passivetotal:
  - user-mail1:api-key1
  - user-mail2:api-key2

trickest:
  - your-api-key1
  - your-api-key2
```

New users will be required to update in the next version if any new resources are added.

5 Examples

5.1 Basic Domain Enumeration

```
subdominator -d example.com
```

5.2 Bulk Enumeration with Output Directory

```
subdominator -dL domains.txt -oD ./results/
```

5.3 JSON Output with All Sources

```
subdominator -d example.com -all -json -o results.json
```

5.4 Custom Google Dork

```
subdominator -d target.com -ir google --dork 'site:target.com -www -dev
    intext:secrets'
```

5.4.1 Advanced Enumeration with Filtering

```
subdominator -d target.com -all -fw -t 60 -o results.txt -V
```

Description: Comprehensive scan using all sources, filtering wildcards, with 60-second timeout, verbose output, and saving to file.

5.4.2 With Proxy for Debugging

```
subdominator -d target.com -px http://127.0.0.1:8080 -s -nc
```

Description: Route traffic through proxy for debugging, silent mode with no colors.

5.4.3 Silent Mode for Automation

```
subdominator -d target.com -s -o subdomains.txt
```

Description: Clean output with only subdomains, perfect for scripting and automation.

5.4.4 Check API Key Status

```
subdominator -d test.com -ir shodan -ski -ls
```

Description: Test Shodan API key functionality and list available sources.

5.5 Most Important One-Line Example

5.5.1 Comprehensive Enumeration Command

```
subdominator -d target.com -all -fw -o subdomains.txt -json
```

Why this is the most important command:

- `-d target.com` - Specifies the target domain for enumeration
- `-all` - Uses all available sources for maximum coverage
- `-fw` - Filters out wildcard subdomains to clean results
- `-o subdomains.txt` - Saves results to a file for persistence
- `-json` - Provides structured data format for further processing

This single command provides the most comprehensive subdomain enumeration with clean, usable output that can be easily integrated into other tools or workflows. It represents the optimal balance between coverage, output quality, and practical utility for bug bounty hunters and security researchers.

NOTE ⇒ Subdominator consistently discovers more subdomains than Subfinder