Subdomain Discovery Quick Reference

Installation

```bash
sudo apt update && sudo apt install knockpy -y
knockpy -h
```

API Configuration

```bash
# Create config file
mkdir -p ~/.config/knockpy
vim ~/.config/knockpy/knockpy.cfg
```

Config File Format

```ini
[virustotal]
api_key = your_api_key_here

[shodan]
api_key = your_api_key_here

[censys]
api_id = your_censys_id
api_secret = your_censys_secret
```

Basic Commands

```bash
```

```
# Basic scan
knockpy example.com

# With APIs
knockpy example.com --use-api

# Custom wordlist
knockpy example.com -w /usr/share/wordlists/

# Filter wildcards
knockpy example.com --no-http

# Save results
knockpy example.com --output my_scan.json
```

Analyze Results

bash

```
# View JSON
cat my_scan.json | jq .

# Check if live
curl -I http://sub.example.com
```

Troubleshooting

- No results? Try different wordlist or VPN
- Config issues? Check `~/.config/knockpy/knockpy.cfg`