Pentesting0x

Knockpy

START

By: sudobyter

What's Knock ?

Knockpy is a powerful Python tool designed for the enumeration of subdomains to uncover potential security vulnerabilities. It's ideal for security professionals, penetration testers, and bug bounty hunters.

Knockpy هي أداة قوية مبنية بلغة Python مصممة لتعداد النطاقات الفرعية
لكشف الثغرات الأمنية المحتملة. إنها مثالية للمحترفين الأمنيين واختبار الاختراق
وصائدي الجوائز.

How to install Knockpy?

- Python pip

```
$_>pip install knockpy
```

Examples of using Knock?

Basic Enumeration

```
$_> knockpy example.com
```

Saving Results

```
$_> knockpy example.com -o output.txt
```

Examples of using Knock?

- ## Using Custom Wordlist

```
$_> knockpy example.com -w custom_wordlist.txt
```

- ## Output Formats

```
$_> knockpy example.com -f json
```

Examples of using Knock?

Verbose Mode

```
$_>knockpy example.com -v
```

With API key (Example API)

```
$_>knockpy domain.com --api APIKEY
```

Examples of using Knock?

- Filtering Results

```
$_> knockpy domain.com -f csv | grep -v 'exclude-pattern
```

- Scheduled Scanning (using cron job)

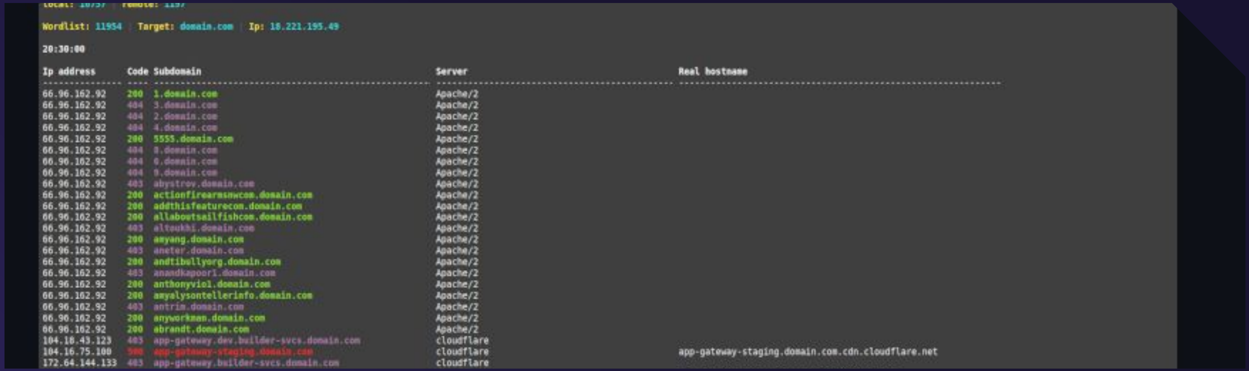
```
$_> (crontab -l 2>/dev/null; echo "0 0 * * * /usr/local/bin/knockpy
domain.com -o /path/to/output-$(date +\%F).txt") | crontab -l
```

aliwaleedhum

Github Knock

URL

https://github.com/guelfoweb/knock



```
Local: 10757 | remote: 1197

Wordlist: 11954 | Target: domain.com | Ip: 18.221.195.49

20:30:00

Ip address      Code Subdomain                                  Server                         Real hostname
--------------- ---- ------------------------------------------ ------------------------------ ------------------------------------------------
66.96.162.92    200  1.domain.com                               Apache/2
66.96.162.92    404  3.domain.com                               Apache/2
66.96.162.92    404  2.domain.com                               Apache/2
66.96.162.92    404  4.domain.com                               Apache/2
66.96.162.92    200  5555.domain.com                            Apache/2
66.96.162.92    404  8.domain.com                               Apache/2
66.96.162.92    404  6.domain.com                               Apache/2
66.96.162.92    404  9.domain.com                               Apache/2
66.96.162.92    403  abystrov.domain.com                        Apache/2
66.96.162.92    200  actionfirearmsnwcom.domain.com             Apache/2
66.96.162.92    200  addthisfeaturecom.domain.com               Apache/2
66.96.162.92    200  allaboutsailfishcom.domain.com             Apache/2
66.96.162.92    403  altoukhi.domain.com                        Apache/2
66.96.162.92    200  amyang.domain.com                          Apache/2
66.96.162.92    403  aneter.domain.com                          Apache/2
66.96.162.92    200  andtibullyorg.domain.com                   Apache/2
66.96.162.92    403  anandkapoor1.domain.com                    Apache/2
66.96.162.92    200  anthonyviol.domain.com                     Apache/2
66.96.162.92    200  amyalysontellerinfo.domain.com             Apache/2
66.96.162.92    403  antrim.domain.com                          Apache/2
66.96.162.92    200  anyworkman.domain.com                      Apache/2
66.96.162.92    200  abrandt.domain.com                         Apache/2
104.18.43.123   403  app-gateway.dev.builder-svcs.domain.com    cloudflare
104.16.75.100   500  app-gateway-staging.domain.com             cloudflare                     app-gateway-staging.domain.com.cdn.cloudflare.net
172.64.144.133  403  app-gateway.builder-svcs.domain.com        cloudflare
```

aliwaleedhum

Y0U C4N
F1ND M3 @T

https://aliwaleed.xyz

sudobyter@gmail.com