Knockpy 4.1.1 Cheatsheet (ingenieriainformatica.uniovi.es)

Enumerates subdomains on a target domain through a wordlist

https://github.com/guelfoweb/knock

GENERAL USAGE

```
knockpy [-h] [--version] [-w WORDLIST] [-r] [-c] [-f] [-j] domain
```

NOTES

For virustotal subdomains support you can setting your API KEY in the config.json file.

OPTIONS

POSITIONAL ARGUMENTS

domain: target to scan, like domain.com

OPTIONAL ARGUMENTS

-c, --csv: save output in csv

-f, --csvfields: add fields name to the first row of csv output file

-h, --help: show this help message and exit

-j, --json: export full report in JSON

-r, --resolve: resolve single ip or domain name

--version: show program's version number and exit

-w WORDLIST: specific path to wordlist file

EXAMPLES

knockpy domain.com

knockpy domain.com -w wordlist.txt

knockpy -r domain.com or IP

knockpy -c domain.com

knockpy -j domain.com

by José Manuel Redondo López

```
operario@kali:~$ knockpy uniovi.es

 _ __                _
| |/ /              | |   4.1.1
| ' / _ __   ___   __| | ___ __  _   _
|  < | '_ \ / _ \ / _| |/ / '_ \| | | |
| . \| | | | (_) | (_|   <| |_) | |_| |
|_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                           | |     __/ |
                           |_|    |___/

+ checking for virustotal subdomains:SKIP
        VirusTotal API_KEY not found
+ checking for wildcard:NO
+ checking for zonetransfer:NO
+ resolving target:YES
- scanning for subdomain ...

Ip Address      Status  Type    Domain Name                     Server
──────────      ──────  ────    ───────────                     ──────
156.35.225.5            alias   acceso.uniovi.es
156.35.225.5            host    acceso05.si.uniovi.es
156.35.33.106           alias   agenda.uniovi.es
156.35.33.106           host    agenda.innova.uniovi.es
156.35.46.123   302     host    api.uniovi.es
156.35.45.90    200     alias   cms.uniovi.es
156.35.45.90    200     host    cms.mieres.uniovi.es
156.35.33.105           alias   empresas.uniovi.es
156.35.33.105           host    webunioviedo.innova.uniovi.es
156.35.23.24    302     alias   ftp.uniovi.es
156.35.23.24    302     host    zeus.etsimo.uniovi.es
156.35.91.31            alias   gopher.uniovi.es
156.35.91.31            host    gustavo.ccu.uniovi.es
156.35.11.177           alias   hermes.uniovi.es
156.35.11.177           host    hermes.net.uniovi.es
156.35.233.100  301     host    intranet.uniovi.es
156.35.152.5    200     alias   isa.uniovi.es
156.35.152.5    200     host    hecate.edv.uniovi.es
45.55.72.95     301     alias   mail.uniovi.es
45.55.72.95     301     host    alias.redirect.name
```