User manual:

Requirements to install:

1. OS: Linux 64 bit
2. Python3
3. Go language latest or >1.14

Steps to install:

1.
   ```
   sudo apt install python3 python3-pip git curl libpcap-dev wget python3-dev python3-dnspython pv dnsutils build-essential libssl-dev libffi-dev libxml2-dev libxslt1-dev zlib1g-dev nmap python3-shodan apt-transport-https   -y
   ```
2. install go from site and configure path
3. after this go to .bashrc or .zshrc file and add these lines at the end of the file.

```
export GOROOT=/usr/local/go

export GOPATH=$HOME/go

export PATH=$GOPATH/bin:$GOROOT/bin:$PATH
```

Installing tools:

1. findomain :

   ```
   wget -N -c https://github.com/Edu4rdSHL/findomain/releases/latest/download/findomain-linux
   sudo mv findomain-linux /usr/local/bin/findomain
   sudo chmod 755 /usr/local/bin/findomain
   wget -nc -O ~/.config/amass/config.ini https://raw.githubusercontent.com/OWASP/Amass/master/examples/config.ini
   ```

```
2. go get  -v github.com/tomnomnom/qsreplace
3. GO111MODULE=on go get -v  github.com/OWASP/Amass/v3/
4. go get  -v github.com/tomnomnom/assetfinder
5. go get -v github.com/tomnomnom/hacks/waybackurls
6. go get -v github.com/tomnomnom/anew
7. go get -v github.com/tomnomnom/unfurl
8. GO111MODULE=on go get -v github.com/projectdiscovery/httpx/cmd/httpx
9. GO111MODULE=on go get -v github.com/projectdiscovery/subfinder/v2/cmd/subfinder
10.    GO111MODULE=on go get -u -v github.com/bp0lr/gauplus
11.    go get -v github.com/cgboal/sonarsearch/crobat

12.    GO111MODULE=on go get -v github.com/projectdiscovery/nuclei/v2/cmd/nuclei

13.    eval git clone https://github.com/projectdiscovery/nuclei-templates ~/nuclei-templates

14.    eval nuclei -update-templates

15.    eval sed -i 's/^miscellaneous/#miscellaneous/' ~/nuclei-templates/.nuclei-ignore

16.    eval sed -i 's/^#random-agent: false/random-agent: true/' ~/.config/nuclei/config.yaml

17.    eval wget -O resolvers_trusted.txt https://gist.githubusercontent.com/six2dez/ae9ed7e5c786461868abd3f2344401b6/raw
```

18. mkdir ~/Tools; git clone https://github.com/darkoperator/dnsrecon.git ~/Tools/dnsrecon/;python3 ~/Tools/dnsrecon/setup.py

19. GO111MODULE=on go get -v github.com/projectdiscovery/nuclei/v2/cmd/nuclei

20. eval git clone https://github.com/projectdiscovery/nuclei-templates ~/nuclei-templates

21. eval sed -i 's/^miscellaneous/#miscellaneous/' ~/nuclei-templates/.nuclei-ignore

22. eval sed -i 's/^#random-agent: false/random-agent: true/' ~/.config/nuclei/config.yaml

23. eval git clone --depth 1 https://github.com/drwetter/testssl.sh.git ~/Tools/testssl.sh ;

24. pip3 install multithreading termcolor sys os colored subprocess readline art

25. git clone https://github.com/six2dez/degoogle_hunter.git ~/Tools/degoogle_hunter

26. git clone https://github.com/obheda12/GitDorker.git ~/Tools/GitDorker

27. git clone https://github.com/s0md3v/Corsy.git ~/Tools/Corsy

28. git clone https://github.com/Tuhinshubhra/CMSeeK.git ~/Tools/CMSeeK

At the end of everything to strip libraries of go :

```
eval strip -s $HOME/go/bin/*
```

Or Just refer to ./install.sh

Configuring shodan and other api keys:

Command: shodan init <api-key>

Edit ~/.config/amass/config.ini this file and enter api keys.

findomain_<name_of_api_>_token=”Your access token” findomain-(options)

For example : findomain_virustotal_token="YourAccessToken" findomain -(options)

How to use the framework:

Command: python3 recon-tool.py

Then type “1” for entering target domain

Then type “2” for entering output directory

Then type “3” for commencing recon. Done