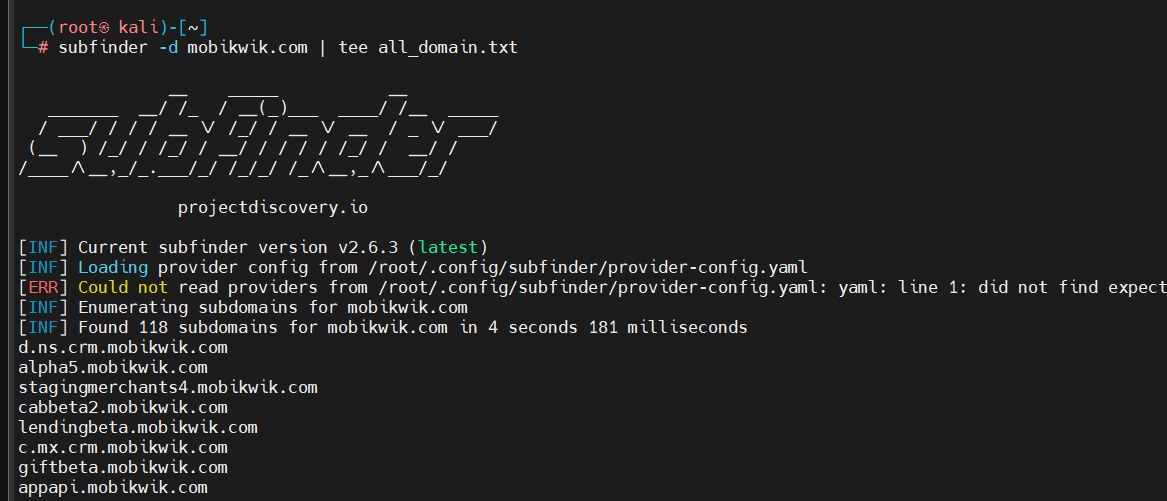
Now, In this practical, we have to find subdomains of a target website.

We will use various tools to collect domains.

Tools: subfinder,amass, amass,assetfinder,finddomain,

Internet Archieve: Waybackurls,gauplus

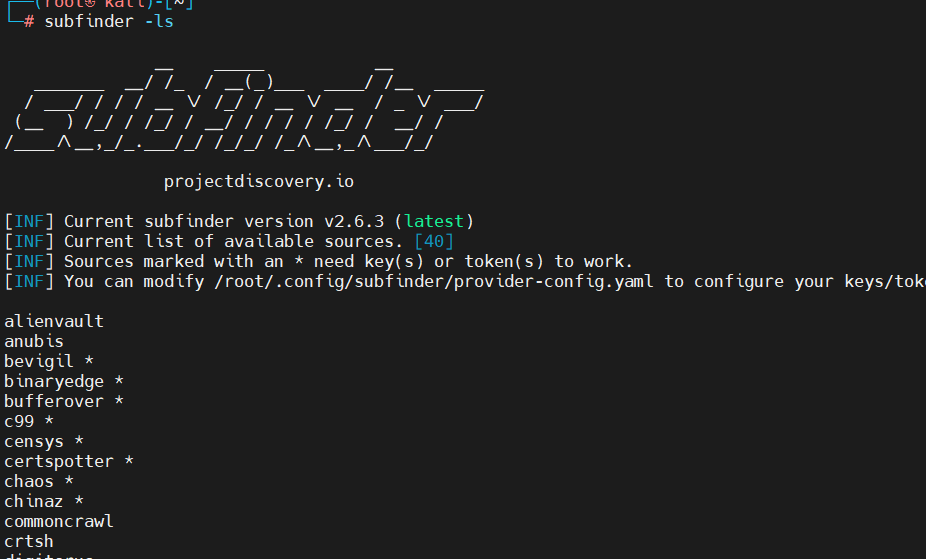
To install all above software, go is prerequisite.

Subfinder:-

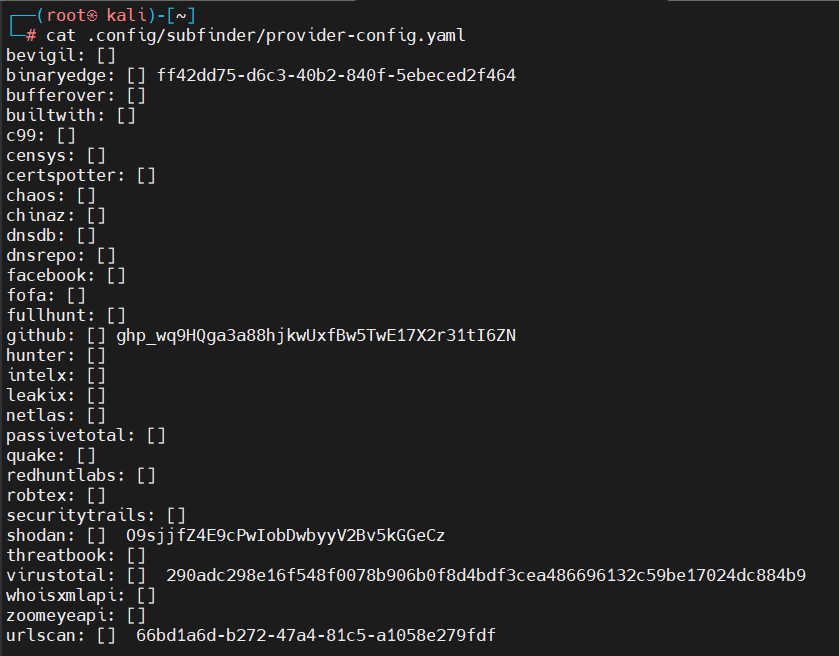
subfinder -d mobikwik.com | tee all\_domain.txt

-d : Domain

This all are no-authenticated results. To get authenticated result. We have to api key to config file.

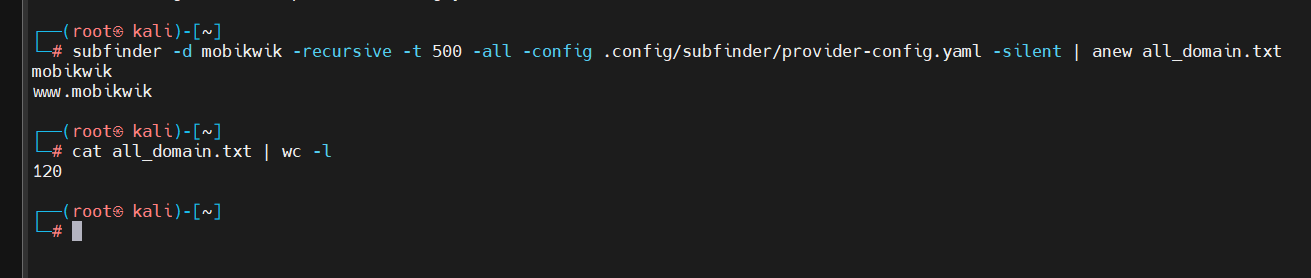
The above command will list sources.

We added some api keys in config file

Now, We have to install anew tool. anew is same like tee command. The only difference is, anew will add data in existing file only if data is new.

To install a new:-

#go install -v github.com/tomnomnom/anew@latest



# subfinder -d mobikwik -recursive -t 500 -all -config .config/subfinder/provider-config.yaml -silent | anew all\_domain.txt

-t: threads

-config : Location of config file

=======================================================================

Now we will try to find subdomain using amass tool:

To install amass:

go install -v [github.com/owasp-amass/amass/v4/...@master](mailto:github.com/owasp-amass/amass/v4/...@master)

Not getting output: will try other tool

Tool: findomain tool

Installation:-

# curl -LO <https://github.com/findomain/findomain/releases/latest/download/findomain-linux.zip>

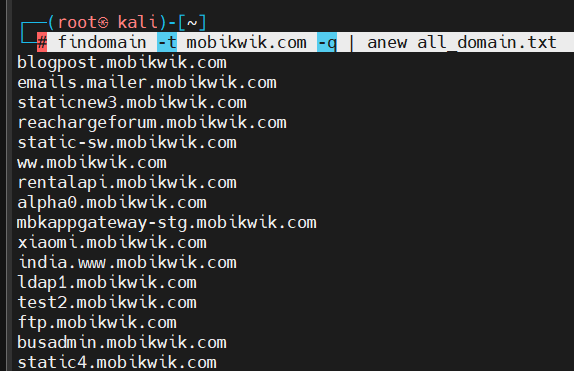
$ unzip findomain-aarch64.zip

$ chmod +x findomain

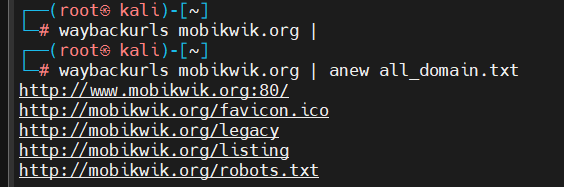
$ sudo mv findomain /usr/bin/findomain

$ findomain –help

------------------

# findomain -t mobikwik.com -q | anew all\_domain.txt

Wayback urls:-

go install github.com/tomnomnom/waybackurls@latest

Gauplus:-

Httpx: tool

go install -v github.com/projectdiscovery/httpx/cmd/httpx@latest