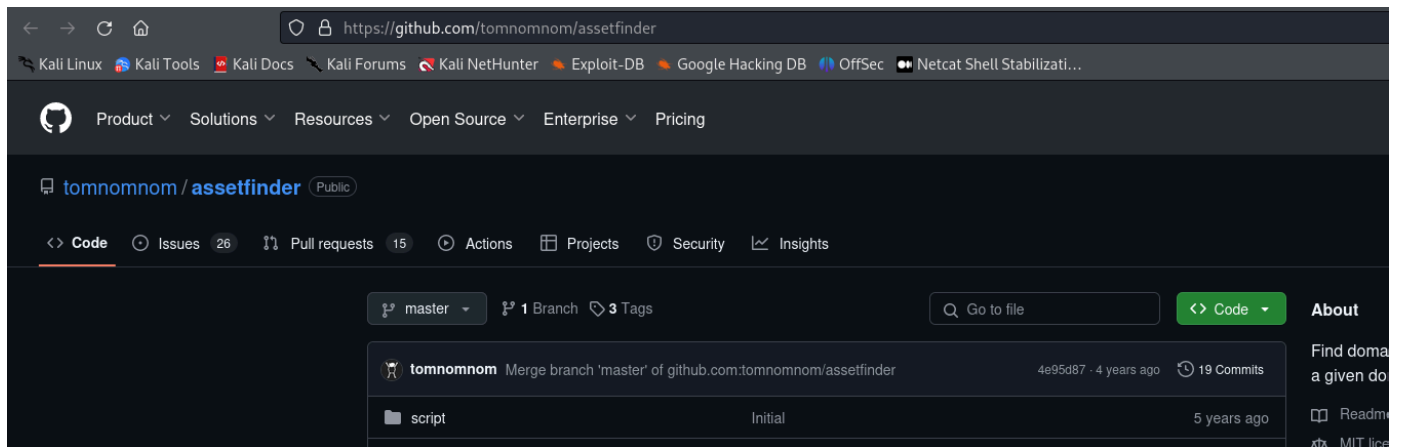


02 - Assetfinder - Finding Subdomains



<https://github.com/tomnomnom/assetfinder>

Stay tuned with this account.

The repo gives the command to install the tool.

"#go get -u github.com/tomnomnom/assetfinder" this does not work anymore. IT DOES NOT WORK ANYMORE

Instead use:

"#go install github.com/tomnomnom/assetfinder@latest" This one works as of 11/11/2024.

Now, we can run assetfinder command.

"#assetfinder tesla.com "

If we only want information from that subdomain, we can use:

"#assetfinder --subs-only tesla.com"

Now, we are going to create a script to run the #assetfinder command, grep the subdomain related info only, and write the output to a file:

The script:

...

#!/bin/bash

url = \$1

```
if [ ! -d "$url" ]; then
    mkdir
```

KaTeX parse error: Undefined control sequence: \[at position 11: url fi if \underline! -d "

KaTeX parse error: Undefined control sequence: \[at position 15: url fi if \underline! -d "

```
url/recon" ]; then
    mkdir $url/recon
fi
```

```
echo "[+] Harvesting subdomains with assetfinder..."
assetfinder $url >> $url/recon/assets.txt
cat $url/recon/assets.txt | grep $1 >> $url/recon/final.txt
rm $url/recon/assets.txt
```

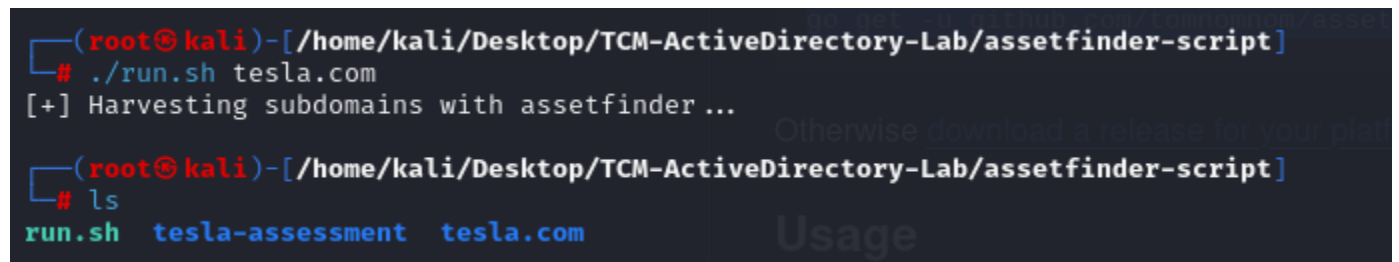
...

After generating the script, we need to run chmod:

```
"#chmod +x run.sh"
```

To run:

```
"#./run.sh tesla.com"
```



```
(root@kali)-[/home/kali/Desktop/TCM-ActiveDirectory-Lab/assetfinder-script]
# ./run.sh tesla.com
[+] Harvesting subdomains with assetfinder ...
Otherwise download a release for your platform

(root@kali)-[/home/kali/Desktop/TCM-ActiveDirectory-Lab/assetfinder-script]
# ls
run.sh  tesla-assessment  tesla.com
Usage
```

It works.

Next step, we are going to use the list generated, or the output of the assetfinder command, to run another tool and see which subdomains are alive. Which is very important information to find out.