04 - Httprobe - Finding Alive Domains

The author of the tools is tomnomnom again.

We can search for result in github.

This is another Go tool.

To install we can run:

"#go install github.com/tomnomnom/httprobe@latest"

We can just cat out the final.txt file, and pipe that to httprobe. The domains that reply are the ones that are alive.

Just like this:

```
┌──(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/assetfinder-script]
└─$ cat tesla.com/recon/final.txt | httprobe
https://dal11-gpgw1.tesla.com
https://ams13-gpgw1.tesla.com
```

-s removes all the default ports.

-p listen on 443

We are going to be making both http, and https requests.

We can run:

"#

cat tesla.com/recon/final.txt | httprobe -s -p https:443 | sed 's/https\?:\/\//' | tr -d ":443""

This will give us only the alive domains.

```
┌──(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/assetfinder-script]
└─$ cat tesla.com/recon/final.txt | httprobe -s -p https:443 | sed 's/https\?:\/\///' | tr -d ":443"
dal11-gpgw1.tesla.com
ams1-gpgw1.tesla.com
iad05-gpgw1.tesla.com
hnd1-gpgw1.tesla.com
feedback.tesla.com
sin05-gpgw1.tesla.com
apigateway-message-center-ownership.tesla.com
business-ui-ownership.tesla.com
logcollector-ext.tesla.com
partners.tesla.com
digitalassets.tesla.com
warehouse.tesla.com
toolbox.tesla.com
engage.tesla.com
engage.tesla.com
logcollection.tesla.com
link.tesla.com
sso.tesla.com
mfs-supplier-gfb-stg.tesla.com
secure-static-assets.tesla.com
vmanage-alerts.tesla.com
```

sed is a command that can handles text files and strings. There are many tasks we can perform with this tool.

Now, we are going to be implementing on the script

```
┌──(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/assetfinder-script]
└─$ sudo ./run.sh tesla.com
[sudo] password for kali:
[+] Harvesting subdomains with assetfinder...
[+] Probing for alive domains...

┌──(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/assetfinder-script]
└─$ ls
run.sh  tesla-assessment  tesla.com

┌──(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/assetfinder-script]
└─$ cat tesla.com/recon/alive.txt
digitalassets.tesla.com
dal11-gpgw1.tesla.com
engage.tesla.com
engage.tesla.com
feedback.tesla.com
business-ui-ownership.tesla.com
apigateway-message-center-ownership.tesla.com
ams1-gpgw1.tesla.com
iad05-gpgw1.tesla.com
link.tesla.com
hnd1-gpgw1.tesla.com
logcollector-ext.tesla.com
mfs-supplier-gfb-stg.tesla.com
logcollection.tesla.com
partners.tesla.com
sso.tesla.com
secure-static-assets.tesla.com
toolbox.tesla.com
sin05-gpgw1.tesla.com
warehouse.tesla.com
vmanage-alerts.tesla.com

┌──(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/assetfinder-script]
└─$
```

```

#!/bin/bash

url=$1

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

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

#echo "[+] Harvesting subdomains with Amass..."
#amass enum -d $url >> $url/recon/f.txt
#sort -u $url/recon/f.txt >> $url/recon/final.txt
#rm $url/recon/f.txt

echo "[+] Probing for alive domains..."
cat $url/recon/final.txt | sort -u | httprobe -s -p https:443 | sed 's/https\?:\/\//' | tr -d ":443" >>
$url/recon/alive.txt

```

Now, we can go and enumerate these. We can do some greps to see if we find a something that jumps the eye.