

# Forum: [Hack Forums](#)

Thread: [Websites RECON !!](#)

Th3GodFather - July 23, 2023, 12:56 am

RECON AND GET MORE INFO ABOUT YOUR TARGET fire

- 1 -use Dig: Stands for Domain Information Groper , Dns lookup by querying name servers and displaying the result to you!! ( dig target.com)
- 2- GoBack In Time -> To see Old Files Like robots.txt and urls ( search for tool in github or visit their website )

## SUB-DOMAINS DISCOVER

-> gobuster dir -w /usr/share/wordlists/dirb/common.txt -u target.com

-> Sublist3r usage : python sublis3r.py -d target.com -p 80 443 GITHUB LINK

-> KnockPy Usage: ./knockpy target.com GITHUB LINK

## GOOGLE DORK

site:target.com -site [www.target.com](http://www.target.com)

ONLINE DNS TOOLS LIKE :

<https://dnsdumpster.com/>

<https://searchdns.netcraft.com/>

BONUS fire : <https://github.com/infosec-au/altdns>

Usage: ./altdns.py -i subdomains.txt -o data\_output -w words.txt -r -s output.txt

SUBDOMAIN VALIDATION :

--> <https://github.com/RedSiege/EyeWitness>

provide a list of all subdomains and it will give you like a report with screenshots of all sub-domain

Usage: ./EyeWitness.py -f subdomain.txt

BONUS ++ brain :

--> Censys: is another great online tool that will give you juicy information about your target!!

censys.io: <https://censys.io/>

--> Photon: is basically a data extraction tool which helps us find many useful information from the websites.

Usage: python3 photon.py -u target.com — keys — dns

Download: <https://github.com/s0md3v/Photon>

Good Luck?

anihil - July 23, 2023, 1:55 am  
thanks in advance . sir

PITI - July 23, 2023, 9:25 am

```
gobuster vhost -u domain.com -w awesome_wordlist.txt -v
amass -active -brute -o hosts.txt -d domain.com
curl -s "https://www.virustotal.com/ui/domains/HOST/subdomains?limit=40" | grep -Po
"((http|https):VV)?(([\w.-]*)\.([\w]*)\.([A-z]))\w+" | sort -u
curl https://sonar.omnisint.io/subdomains/domain.com
curl -s https://dns.bufferover.run/dns?q=.HOST.com | jq -r .FDNS_A[] | cut -d',' -f2 | sort -u
gau --subs domain.com | unfurl -u domains
gau --subs domain.com | cut -d "/" -f 3 | sort -u
```

---

FUZZ: ?

```
feroxbuster --url https://www.DOMAIN.com/ -w ~/tools/Wordlists/fuzz.txt --silent -s 200 301 302
--redirects --methods POST,GET,PUT,PATCH,DELETE -k
gobuster -u <targetip> -w /usr/share/seclists/Discovery/Web_Content/common.txt -s
'200,204,301,302,307,403,500' -e
gobuster dir -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt -t
100 -x txt,php,csv,md,json,js,html,py,sh -u http://domain
wfuzz -c -w /usr/share/seclists/Fuzzing/LFI/LFI-LFISuite-pathtotest-huge.txt --hc 404 --hh 206
http://domain/index.php?file=FUZZ
```

Th3GodFather - July 23, 2023, 5:39 pm

(Jul 23, 2023 09:25 AM)PITI Wrote: [CITE](#) gobuster vhost -u domain.com -w awesome\_wordlist.txt -v

```
amass -active -brute -o hosts.txt -d domain.com
curl -s "https://www.virustotal.com/ui/domains/HOST/subdomains?limit=40" | grep -Po
"((http|https):VV)?(([\w.-]*)\.([\w]*)\.([A-z]))\w+" | sort -u
curl https://sonar.omnisint.io/subdomains/domain.com
curl -s https://dns.bufferover.run/dns?q=.HOST.com | jq -r .FDNS_A[] | cut -d',' -f2 | sort -u
gau --subs domain.com | unfurl -u domains
gau --subs domain.com | cut -d "/" -f 3 | sort -u
```

---

FUZZ: ?

```
feroxbuster --url https://www.DOMAIN.com/ -w ~/tools/Wordlists/fuzz.txt --silent -s 200 301 302
--redirects --methods POST,GET,PUT,PATCH,DELETE -k
gobuster -u <targetip> -w /usr/share/seclists/Discovery/Web_Content/common.txt -s
'200,204,301,302,307,403,500' -e
gobuster dir -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt -t
100 -x txt,php,csv,md,json,js,html,py,sh -u http://domain
wfuzz -c -w /usr/share/seclists/Fuzzing/LFI/LFI-LFISuite-pathtotest-huge.txt --hc 404 --hh 206
http://domain/index.php?file=FUZZ
```

Thank you I will Add that to my experience