

Recon

Amass Intel `amass intel -active -p 80,81,443,59-1,2082,2087,2095,2096,3000,800-0,8001,8008,8080,8083,8443,883-4,8888 -config /root/amass/config.ini -whois -d <DOMAIN>`

Amass Subs (Passive/-Quick) `amass enum -passive -df ./domains.txt -config /root/amass/config-passive.ini`

Amass Subs (Active/S-lower/Thorough) `amass enum -active -brute -w /root/dns_lists/all.txt -df ./domains.txt -config /root/amass/config.ini -o ./amass_results.txt -p 80,443,800,8080,8443 -dir ./amass`

Reverse Subdomains Lookup `https://viewdns.info/reversewhois/?q=<ORGANISATION_NAME>`

Google Dork `site:*.*.<EXAMPLE>.com`

GitHub Search (@gwen001, <GIT_API_TOKEN> -d "\$d"; done git repo)

```
for d in $(cat parent_domains.txt);
do python3 ./github-endpoints.py -t
<GIT_API_TOKEN> -d "$d"; done
```

GAU GetAllUrls (bash loop over)

```
for d in $(cat domains.txt); do
getallurls "$d"; done | tee -a getall-
urls.txt
```

ffuf Magic

```
Ffuf      ssh -nNTvR 9090:localhost:
tunnel    st:8081 root@<IP>

ffuf <COMMAND> -replay-proxy
http://localhost:9090
```



By **dadadarand123**

Not published yet.
Last updated 15th July, 2020.
Page 1 of 1.

Sponsored by **Readable.com**
Measure your website readability!
<https://readable.com>