general notes

Eyad Islam El-Taher

Friday, October 3, 2025

Subdomain Enumeration

- **Knock Subdomain Scan**

```
knockpy -d "domain.com" --recon --bruteforce
```

- **subfinder Scan**

```
subfinder -d someweb.com -o subf.txt -v
```

- **assetfinder Scan**

```
assetfinder -subs-only someweb.com > asset.txt
```

- **Subdomain Finder**

```
https://subdomainfinder.c99.nl/
Save output to a file "subfinder.txt"
```

- **Add all Enumerated/Collected subdomains from different tools in different files into one file with unique subdomains**

```
 cat subf.txt subfinder.txt asset.txt | sort -u > subdomains.txt
```

- **To check the live subdomains and checking the status code of them**

```
cat subdomains.txt | httpx -title -wc -sc -cl -ct -location -web-server
-o alive-subdomains.txt
```