Cheat sheet / Tools

Root Domains Enumeration:

- Crunchbase (acquisitions)
- Trademarks (google fu)
- Chatgpt
- Favicons (hash generator then shodan)
- whois
- viewdns.info (email)
- reverse whois
  - `amass intel -whois -d google.com`
- TLD Hunt (tries all .com/.org ...)
  - `tldhunt -k <org> -E tlds.txt`

CIDR Recon:

- http://bgp.he.net (manual)
- metabigor
  - `echo facebook | metabigor net --org -o result.txt`
  - `echo AS54115 | metabigor net --asn -o result.txt`
- ASNLookup
- asnmap

Passive Subdomain Enumeration:

`echo <cidr> | dnsx -silent -resp-only -ptr`

- Virusttotal (relations)
- Github/Gitlab Subdomains
- Waybackurls

```
waybackurls > urls.txt
sed -E 's#^(https?://)?([^/]+).*#\2#' urls.txt | sort -u
```

- Subfinder
  - `subfinder -d facebook.com`
  - `sudomy -d facebook.com`

Active Subdomain Enumerations:

- gobuster
  - `gobuster dns -d apple.com -w <wordlist.txt`

Tech Stack Enumeration:

- whatweb (website and tool)
  - `whatweb -a3 https://facebook.com -v`
- httpx
  - `httpx -l listofUrls.txt -v` # List live
  - `httpx -l listofUrls.txt -td` # List with tech
- wappalyzer (browser extension)
- wafw00f (for web application firewall)
  - `wafw00f -v https://google.com`

Screenshotting Assets:

- aquatone
  - `cat screenshots.txt | aquatone`

Google Dorks:

- Google Fu
- Google Hacking DataBase
- Ahmed Faisal Dorks

Shodan:
https://github.com/jakejarvis/awesome-shodan-queries

- shosubgo (needs api, free)
  - `shosubgo -d ibm.com -s <token>`
- smap (similar to nmap, but uses shodan, also needs token)

Github Dorking:

org:ibm "ssh"

trufflehog, automated searching (supply with repo, get open secrets)

Cloud:

- aws client
  - `aws s3 ls s3://bucketName`
  - `aws s3 cp s3://bucketName/fileName destination`

> You can add `--no-sign-request` for aws commands

- cloud_enum (finds aws services for a domain)

hunter.io

looks up emails in an organization

apivoid

checks reputation of email

Breach Cheks:

- DeHashed
- Haveibeenpwned

Reverse Image Lookup

- images.google.com

image exif data

- exiftool