INFORMATION GATHERINGS

1. Crt.sh

Ye ek Certificate Transparency log search engine hai.

Jab bhi kisi domain/subdomain ke liye SSL certificate banaya jata hai, uska record publicly log hota hai.

2. Amass

Ye ek powerful open-source tool hai jo DNS enumeration, scraping, brute force aur OSINT methods ka use Karta hai

3. Subfinder & ffuf

Subfinder: Ek fast passive subdomain discovery tool hai (projectdiscovery ka). Ye APIs aur public datasets ka use karke subdomains nikalta hai.

ffuf (Fuzz Faster U Fool): Ye ek fuzzing tool hai. Tum isse subdomain brute-forcing ya directory brute-forcing kar sakte hai

4. Sort & anew – Duplicate

Jab tum alag-alag tools ka output lete ho, toh duplicate subdomains aa jate hain.

sort aur anew commands use karke tum list ko clean karte ho:

5. Sublister & httpx/httpprobe

Sublist3r (Sublister): Ek Python-based tool hai jo search engines (Google, Bing, Yahoo, Baidu) se subdomains extract karta hai.

httpx/httpprobe: Ye ek HTTP probing tool hai jo check karta hai ki subdomain live hai ya dead.

httpx (ProjectDiscovery ka) zyada advanced Sublister = subdomains nikalna.

6. Chaos & Eyewitness

Chaos: ProjectDiscovery ka ek database hai jisme verified domains aur subdomains store hote hain (bug bounty ke liye kaafi useful).

Eyewitness: Ye ek tool hai jo screenshots capture karta hai subdomains ke web pages ka, aur ek HTML report banata hai.

🔗 Overall Workflow Example

1. crt.sh, amass, subfinder, sublister → Subdomains collect karna

2. sort | anew → Clean & unique list banana.

3. httpx/httpprobe → Live subdomains filter karna.

4. ffuf → Brute force se hidden subdomains/directories find karna.

5. chaos → Extra data fetch karna.

6. eyewitness → Live domains ka screenshot aur report banana.

7. SecretFinder

A Python script that scans JavaScript files to detect API keys, tokens, credentials, and sensitive information.

Uses regex patterns to find hidden secrets.

Example: Finding AWS keys, Google API keys inside JS files.

python3 SecretFinder.py -i https://target.com/file.js -o cli

subfinder -d target.com -o subdomains.txt

8. Katana

A fast crawler made by ProjectDiscovery.

Collects URLs from websites by crawling links, sitemaps, and responses.

Useful for extracting .js files or hidden endpoints.

katana -u https://target.com -o allurls.txt

9. getJS

A tool to fetch JavaScript file URLs from a target.

Helps automate the process of finding linked JS files from HTML pages or responses.

10. Nuclei

A vulnerability scanner based on templates(YAML rules).

You can use it to scan discovered subdomains, endpoints, and JS files for known misconfigurations, CVEs, or exposures.

Example: nuclei -l urls.txt -t cves/

11. Mantra

A framework for JS analysis and security automation.

Helps in extracting endpoints, finding secrets, analyzing JavaScript files, and more.

12. subjs

A small tool that extracts JavaScript file URLs from a list of websites.

Very fast and helpful to collect .js files for further analysis.

13. grep

A Linux command-line utility for searching text using regex.

Often used to filter specific patterns like .js, api, token, key.

```
cat allurls.txt | grep ".js$" | anew jsfiles.txt
```

14. anew

A CLI tool to append new unique lines to a file.

Useful for de-duplication when collecting large sets of URLs.

Example:

```
cat urls.txt | anew final_urls.txt
```

15. GitGraber kya hai –

GitGraber ek automated tool hai jo Git repositories (GitHub, GitLab, Bitbucket, etc.) me sensitive data dhoondhne ke liye use hota hai. Ye basically Git Dorks ka automated version hai – tumhe manually queries daalne ki zarurat nahi hoti, tool khud scan karta hai aur files dhoondhta hai jisme vulnerabilities ho sakti hain.

```
python3 gitGraber.py --target github.com --query "file:.env"
```

16. What is ShuffleDNS?

ShuffleDNS is a fast subdomain enumeration tool used mainly in bug bounty hunting, penetration testing, and reconnaissance.

It is part of ProjectDiscovery tools (the same creators of subfinder, httpx, naabu, etc.).

☸ Purpose

It focuses on resolving and brute-forcing subdomains efficiently using massdns-style parallel DNS queries.

In simpler terms:

ShuffleDNS takes a list of possible subdomains and checks which ones actually exist (resolve to an IP).

17. What subdomain takeover

A subdomain takeover is a security vulnerability that occurs when a subdomain (like sub.example.com) points to an external service (like GitHub Pages, AWS S3, Heroku, or Azure) that has been deleted, unclaimed, or misconfigured, allowing an attacker to take control of that subdomain.

In simpler terms:

- Your main domain is example.com.
- You have a subdomain blog.example.com pointing to a service (say, GitHub Pages).
- If that GitHub Pages repository is deleted or never set up properly, the DNS still points to GitHub.
- An attacker can register that GitHub Pages service and now blog.example.com is under their control

18. GitHub Recon ka use kyun hota hai?

Cybersecurity researchers ya bug bounty hunters GitHub recon isliye karte hain:

- Company ke source code leaks dhundhne ke liye
- Hardcoded API keys, tokens, passwords ya secrets nikalne ke liye
- Kisi organization ka tech stack samajhne ke liye
- Past security issues ya commit messages padhkar attack surface samajhne ke liye

---

INFORMATION GATHERINGS

Kaise karte hain GitHub Recon?

1. GitHub pe jaake organization ya user profile dhundho:
    - Example: https://github.com/facebook
    - "rapyd.net" database NOT test NOT example
2. Repositories, commits, branches, issues ko manually check karo.
3. Keywords search karo jaise:
    - password
    - secret
    - AWS_KEY
    - api_key

GitDorker kya karta hai?

GitDorker GitHub ka search API use karke dorks (search queries) run karta hai aur unke results nikalta hai. Example dork:

19.GitGraber kya hota hai?

GitGraber ek OSINT (Open Source Intelligence) tool hai jo GitHub jaise platforms par public repositories me sensitive information leaks (jaise API keys, passwords, tokens, credentials) ko dhoondhne ke liye use hota hai.

Use Case:

Security researchers, bug bounty hunters, aur pentesters GitGraber ka use karte hain taaki:

- Kisi specific domain, email, ya keyword ke against
- GitHub par jo public leaks hain, unhe automatically monitor aur detect kar sakein

20.Target scanning kya hai?

Target scanning ek reconnaissance step hai jo penetration testing aur network security me use hota hai — iska maksad yeh hota hai ke aap kisi target (IP, range, domain, ya web application) ke baare me information ikattha karo jo aage ke testing/attack steps (jaise exploitation) ke liye zaroori hoti hai.

INFORMATION GATHERINGS

- **nmap** — mahaan aur flexible (host discovery, port/service/OS detection).
- **masscan** — bahut fast large-scale port scan.
- **nikto / dirb / gobuster** — web vulnerability and directory brute force.
- **nessus / openvas** — vulnerability scanners with CVE checks.
- **whatweb / wappalyzer** — web tech fingerprinting.
- **httprobe / httpx** — HTTP probe tools for large lists.

-Pn = don't ping before scanning (useful agar host blocks ICMP).
-sS = SYN scan (fast, stealthier).
-sV = service/version detection.
-O = OS detection.
-A = aggressive (enables several checks).

21. What it does — quick list

- **Slice** a big CIDR into smaller blocks (by number of CIDRs or number of hosts).
- **Aggregate / merge** overlapping or adjacent CIDRs into a compact list.
- **Normalize / clean** duplicate or malformed entries.
- **Print / expand** CIDRs (for downstream tools).
- **Script friendly**: supports silent/output flags so you can use it in pipelines.

Why use it

When you get ASN → CIDR outputs, or large/netwide blocks, mapcidr helps you standardize and split them so scanners (nmap, masscan, httpx, etc.) can work efficiently and predictably

22. DNSX — dnsx ek fast DNS probing tool hai jo bahut saare DNS queries ek saath (concurrently) chala sakta hai.

Yeh pentesters / bug-hunters / network engineers ke liye bana hua hai — jab tumhare paas bade lists of domains ya IPs ho aur unke DNS records jaldi check karne ho.

Socho: tumhare paas 1000 IPs ya 10,000 subdomains — manually dig chalana time-consuming hai. dnsx yeh sab parallel (tez) karke clean output deta hai jo scripting/pipelines ke liye perfect hota hai.

(a) Common DNS record types jo dnsx

A — domain ka IPv4 address

AAAA — IPv6 address

CNAME — canonical name / alias

PTR — reverse DNS (IP → hostname)

MX — mail exchange servers (mail handling)

TXT — text records (SPF, DKIM, verification strings)

NS — name servers

23. naabu — naabu ProjectDiscovery ka ek **fast port-scanner** hai jo hosts/IP lists ke open ports jaldi identify karta hai. Yeh TCP SYN/CONNECT aur UDP scans dono support karta hai

use cases

- Bug bounty / attack-surface mapping: jaldi pata lagana kaunse hosts par kaunse ports open hain.
- Recon pipelines: subfinder/amass → naabu → httpx → nuclei.
- Mass scanning across many hosts (VPS/fast network recommended). Medium+1

Khatarnak nahin — lekin dhyaan rakho

Active port scanning target networks par **noticeable** hota hai. Hamesha permission lo (legal/ethical). High speed se target block/blacklist ho sakta hai.

24. Masscan kya hai

Masscan ek bahut tezz TCP port scanner hai jo raw SYN packets bhejta hai. Use case: internet-scale ya large network scans jahan speed zaroori ho. Lekin ye deep service detection nahi karta

— sirf open ports batata hai.