Recon（侦察）

https://infosecwriteups.com/recon-to-master-the-complete-bug-bounty-checklist-95b80ea55ff0

💡 **Multiple**

https://viewdns.info/

https://www.virustotal.com/gui/home/upload

https://securitytoolkits.com/tools/whois

🔍 **WHOIS**

https://whois.domaintools.com

https://hackertarget.com/whois-lookup/

🔍 **DNS**

https://dnsdumpster.com

https://intodns.com/

🔍 **SSL**

https://www.ssllabs.com/ssltest/

🔍 **Reverse IP**

https://www.yougetsignal.com/tools/web-sites-on-web-server/

💡 **ASN nslookup**

https://bgp.he.net/

💡 **google hacking**

https://ght.se7ensec.cn/#

https://pentest-tools.com/information-gathering/google-hacking

💡 **Cyberspace Mapping**

shadan fofa zoomeyes 360Quake Censys Hunter

💡 **Certificate**

https://crt.sh/

initiative

https://sitereport.netcraft.com/

https://pentest-tools.com/alltools#reconnaissance-tools

💡 **Port**

https://hackertarget.com/ip-tools/

https://pentest-tools.com/network-vulnerability-scanning/port-scanner-online-nmap

https://dnschecker.org/port-scanner.php

💡 **CMS**

https://whatcms.org/

https://www.wappalyzer.com/lookup/

💡 **dirb**

https://pentest-tools.com/website-vulnerability-scanning/discover-hidden-directories-and-files

subfinder

Passive Recon(被动信息收集)

特点：不与目标系统直接交互，只查询公开数据源，不会对目标产生流量。

1. 域名、WHOIS、注册信息

▼ **在线工具**

> **https://securitytrails.com/domain（USA）**
>
> **https://lookup.icann.org（USA）**
>
> **https://www.onamae.com/service/whois/(JP)**
>
> **https://whois.jprs.jp/ （JP）**
>
> ---
>
> **https://whois.domaintools.com（USA）**
>
> **https://whois.domaintools.com（USA）**
>
> **https://hackertarget.com/whois-lookup/（AUS）**
>
> **https://viewdns.info/whois/（open）**

---

2. DNS 被动分析

- DNSdumpster（注意：其 DNS 解析属于被动侧，未对目标产生主动探测）
- IntoDNS（配置检查属于被动）
- PassiveDNS 数据库（如某些整合平台）

3. 证书透明度日志

- crt.sh
- Censys Certificates
- Facebook CT logs

4. 网络空间搜索引擎

注意：此类平台搜索本身属于被动，前提是你不触发其“实时扫描”功能。

- Shodan
- FOFA
- ZoomEye
- Quake
- Censys

- Hunter
- Netlas

5. 历史记录与元数据

- Wayback Machine
- Netcraft Site Report
- BuiltWith (技术栈识别)
- Wappalyzer online lookup (被动，不访问目标)
- WhatCMS (部分请求是被动读取数据库)

6. 搜索引擎利用

- Google Dork 工具（ght、pentest-tools Google hacking）
- Bing/Google/Yandex 搜索

7. 公开威胁情报、黑名单、泄露库

- VirusTotal（查询域名/IP 时属于被动）
- ThreatCrowd
- AlienVault OTX
- SecurityTrails（数据库侧）

主动信息收集 Active Recon

特点：工具服务器会对目标发起实际请求。即使访问者是你从 Tor 出去，也属于主动。

1. 在线端口扫描

- pentest-tools online nmap
- DNSChecker port scanner
- HackerTarget IP tools port scan

- yougetsignal reverse IP（部分功能会对目标发起请求）

2. 在线存活探测、指纹探测

- pentest-tools 指纹扫描
- SSL Labs SSL Test（会对目标发起握手、加解密分析）
- Netcraft active checks（可触发主动测试）

3. 在线目录扫描、路径爆破

- pentest-tools directory discovery
- 若干在线 dirscan 工具
- 若干 online fuzzing 端点

4. CMS 扫描

- WhatCMS 深度检测模式
- Wappalyzer active scan
- pentest-tools CMS scanning

5. 在线漏洞扫描器

这些始终是主动：

- pentest-tools 全套扫描
- openvas web 版
- 在线 SQLi/XSS 自动扫描器
- 在线 WAF bypass 测试器

中立（根据你使用的功能而变化）

这些工具有被动功能，也有主动功能，取决于你怎么用。

- VirusTotal（上传样本主动，查询域名被动）

- Netcraft（部分是被动，某些测试项主动）
- SecurityTrails（数据库读取是被动，实时扫描是主动）
- BuiltWith（纯被动）但某些扩展 API 可能触发主动
- Wappalyzer（lookup 为被动，scan 为主动）

DomainTools WHOIS

ViewDNS

HackerTarget WHOIS

SecurityToolkits WHOIS

ICANN Lookup

DomainTools WHOIS

ViewDNS

HackerTarget WHOIS

SecurityToolkits WHOIS

ICANN Lookup