**Tools**

[Altdns](https://github.com/infosec-au/altdns): alternative names brute forcing  
[Amass](https://github.com/caffix/amass): brute force, Google, VirusTotal, alt names  
[aquatone-discover](https://github.com/michenriksen/aquatone): Brute force, Riddler, PassiveTotal, Threat Crowd, Google, VirusTotal, Shodan, SSL Certificates, Netcraft, HackerTarget, DNSDB  
[BiLE-suite](https://github.com/sensepost/BiLE-suite): HTML parsing, alt names, reverse DNS  
[blacksheepwall](https://github.com/tomsteele/blacksheepwall): AXFR, brute force, reverse DNS, Censys, Yandex, Bing, Shodan, Logontube, SSL Certificates, Virus Total  
[Bluto](https://github.com/RandomStorm/Bluto): AXFR, netcraft, brute force  
[brutesubs](https://github.com/anshumanbh/brutesubs): enumall, Sublist3r, Altdns  
[cloudflare\_enum](https://github.com/mandatoryprogrammer/cloudflare_enum): Cloudflare DNS  
[CTFR](https://github.com/UnaPibaGeek/ctfr): SSL Certificates  
[DNS-Discovery](https://github.com/m0nad/DNS-Discovery): brute force  
[DNS Parallel Prober](https://github.com/lorenzog/dns-parallel-prober): DNS resolver  
[dnscan](https://github.com/rbsec/dnscan): AXFR, brute force  
[dnsrecon](https://github.com/darkoperator/dnsrecon): AXFR, zone walking, brute force, reverse DNS, snoop caching, Google  
[dnssearch](https://github.com/evilsocket/dnssearch): brute force  
[domained](https://github.com/reconned/domained): Sublist3r, enumall, Knockpy, SubBrute, MassDNS, recon-ng  
[enumall](https://github.com/jhaddix/domain): recon-ng -> Google, Bing, Baidu, Netcraft, brute force  
[Fierce](https://github.com/mschwager/fierce): AXFR, brute force, reverse DNS  
[Knockpy](http://github.com/guelfoweb/knock): AXFR, virustotal, brute force  
ldns-walk: zone walking (part of package ldnsutils)  
[MassDNS](https://github.com/blechschmidt/massdns): DNS resolver  
[Second Order](https://github.com/mhmdiaa/second-order): HTML parsing  
[Sonar](https://github.com/jrozner/sonar): AXFR, brute force  
[SubBrute](https://github.com/TheRook/subbrute): brute force  
[Sublist3r](https://github.com/aboul3la/Sublist3r): Baidu, Yahoo, Google, Bing, Ask, Netcraft, DNSdumpster, VirusTotal, Threat Crowd, SSL Certificates, PassiveDNS  
[theHarvester](https://github.com/laramies/theHarvester): reverse DNS, brute force, Google, Bing, Dogpile, Yahoo, Baidu, Shodan, Exalead  
TXDNS: alt names (typo/tld)  
[vhost-brute](https://github.com/gwen001/vhost-brute): vhost discovery  
[VHostScan](https://github.com/codingo/VHostScan): vhost discovery  
[virtual-host-discovery](https://github.com/jobertabma/virtual-host-discovery): vhost discovery

**Online DNS tools**

<https://hackertarget.com/>  
<http://searchdns.netcraft.com/>  
<https://dnsdumpster.com/>  
<https://www.threatcrowd.org/>  
<https://riddler.io/>  
[https://api.passivetotal.org](https://api.passivetotal.org/)  
[https://www.censys.io](https://www.censys.io/)  
[https://api.shodan.io](https://api.shodan.io/)  
<http://www.dnsdb.org/f/>  
<https://www.dnsdb.info/>  
<https://scans.io/>  
<https://findsubdomains.com/>  
<https://securitytrails.com/dns-trails>

https://crt.sh/  
<https://certspotter.com/api/v0/certs?domain=example.com>  
<https://transparencyreport.google.com/https/certificates>  
<https://developers.facebook.com/tools/ct>

<https://pentest-tools.com/information-gathering/find-subdomains-of-domain>

<https://intodns.com/>

**Search engines**

<http://www.baidu.com/>  
<http://www.yahoo.com/>  
<http://www.google.com/>  
<http://www.bing.com/>  
<https://www.yandex.ru/>  
<https://www.exalead.com/search/>  
<http://www.dogpile.com/>  
<https://www.zoomeye.org/>  
<https://fofa.so/>

**Technical tools/search engines**

<https://github.com/>  
<https://gitlab.com/>  
<https://www.virustotal.com/fr/>

**DNS cache snooping**

nslookup -norecursive domain.com

nmap -sU -p 53 --script dns-cache-snoop.nse --script-args 'dns-cache-snoop.mode=timed,dns-cache-snoop.domains={domain1,domain2,domain3}' <ip>

**Others online resources**

<https://ask.fm/>  
<http://logontube.com/>  
<http://commoncrawl.org/>  
<http://www.sitedossier.com/>