给出个人目前常用的
其实一些工具，都了很多工作，所以分类就有重复的
1. 子域名
工具子域名看字典，所以选一个方便的一直用就行了
layer，个人的资源链接：
脚本:subDomainsBrute-master
在线的：http://www.youknowi.xin/domain.php
google hacking 找子域名 site:xxx.com

2.
ip:
本地 ping 一下：
爱站的超级 ping：https://dns.aizhan.com
查询网：http://site.ip138.com/
站长之家：http://ip.tool.chinaz.com
kali 的 whatweb 工具：
github 上的 fuckcdn（找真实 ip，常用思路就是找子域名看 c 段）

3.
端口：
直接推荐 nmap 神器，以及 masscan 工具

4.
whois：
还是蛮有用的，对于注册人的信息。
爱站的 whois，kali 的 whois 命令

5.
操作系统的情况：
这个根据一些 web 语言和 web 容器就可以大概判断用的是什么操作系统
云悉：http://www.yunsee.cn/
在线 bugscan：http://whatweb.bugscaner.com/look/
钟馗之眼：https://www.zoomeye.org/
fofa：https://fofa.so/
shodan：https://www.shodan.io/
censys：https://censys.io/

6.
中间件：
这个对于漏洞的检测是非常重要的
云悉：http://www.yunsee.cn/
在线 bugscan：http://whatweb.bugscaner.com/look/

钟馗之眼：https://www.zoomeye.org/
fofa：https://fofa.so/
shodan：https://www.shodan.io/
censys：https://censys.io/

7.
检测是否使用开源源码
尝试公开 poc，exp（可在 github 上搜索）
云悉：http://www.yunsee.cn/
在线 bugscan：http://whatweb.bugscaner.com/look/
钟馗之眼：https://www.zoomeye.org/
fofa：https://fofa.so/
shodan：https://www.shodan.io/
censys：https://censys.io/
这个可以补充一个 md5 库和脚本：
https://github.com/nihaohello/My_Online_Scan/tree/master/scanner/plugins/gwhatcms

8.
服务信息：
检测是否使用开源源码
云悉：http://www.yunsee.cn/
在线 bugscan：http://whatweb.bugscaner.com/look/
钟馗之眼：https://www.zoomeye.org/
fofa：https://fofa.so/
shodan：https://www.shodan.io/
censys：https://censys.io/
再补充 nmap 的脚本和 -sV 参数

9.
目录扫描：
其中包含敏感目录，后台目录，目录 url 等，所以全归在这
扫描看字典：
个人的字典链接：
kali 下 dirb 工具
windows 下的御剑
burpsuite 的爬虫

google haking：
一直使用它，找一些后台，敏感 url
脚本链接（只是处理收集到的，真正的还是要手工）：
https://github.com/nihaohello/web_deal_scripts/tree/master/Get_Urls_From_Google

其他的目前个人并没有多收集什么