信息收集

## 资产信息收集

子域名：

<https://github.com/projectdiscovery/subfinder> 通过接口查询域名，需要配置API KEY

<https://github.com/knownsec/ksubdomain> 接口及字典。速度快，可指定外部字典

./subfinder -d baidu.com -silent|./ksubdomain -verify -silent|./httpx -title -content-length -status-code

<https://github.com/insightglacier/Dictionary-Of-Pentesting>

整理域名字典，分几个数量级

<https://github.com/shmilylty/OneForAll> （需要配置APIkey，接口多）

https://zhuanlan.zhihu.com/p/182584086

<https://github.com/knownsec/Kunyu> 坤宇信息收集，可联动pocsuit3

<https://github.com/kelvinBen/AppInfoScanner> APP的信息收集工具

<https://github.com/zsdevX/DarkEye> 信息收集

<https://github.com/gh0stkey/HaE> burp插件

Whois信息： whois.aliyun.com；whois反查

<http://beian.miit.gov.cn/> 备案网站搜索企业名称

Layer域名爆破：<https://github.com/euphrat1ca/LayerDomainFinder>

子域名的枚举： <https://github.com/aboul3la/Sublist3r>，用法：sublist3r.py -d 100tal.com -t 10。

在线爆破：<http://scan.javasec.cn/>

https://github.com/knownsec/Kunyu

## 信息泄露类漏洞

关键词：smtp,pass,password,svn,git，ftp:密码，内部，token，AccessKey，ak,secret,admin,后台，filename：.sql,.csv,

## 框架指纹识别

<https://github.com/s7ckTeam/Glass> 指纹识别

浏览器插件 wappalyzer

云溪指纹：<http://www.yunsee.cn/>。(需要邀请码账号)

http://whatweb.bugscaner.com/look/

Whatweb：<https://github.com/urbanadventurer/WhatWeb>。

备注方法：whatweb -v -a 3 domain.com

<https://github.com/TideSec/TideFinger>

python3 TideFinger.py -u https://aido.aido.pub/login

<https://github.com/EASY233/Finger>

python3 Finger.py -u aido.aido.pub/login

更多工具见 <https://github.com/knownsec/404StarLink2.0-Galaxy/blob/master/TOOLS_README.md#zsdevxdarkeye> 各测试人员按自己情况使用

## 常见服务漏洞

Nmap：nmap -T4 -A -v -p- IP

<https://github.com/ybdt/dict-hub>

<https://github.com/gh0stkey/Web-Fuzzing-Box>

安全设备  
路由器  
这类漏洞你文档里面好像没有  
  
邮件钓鱼  
社工  
  
密码共用,撞库  
  
企业最薄弱的环节是员工的电脑和内网  
  
员工电脑一般都是win7  
使用的office为老旧版本  
浏览器访问不规范,不升级  
好奇心重  
侥幸心理强  
  
APT攻击屡试不爽就是因为这些原因  
  
而很少直接通过网站攻破  
  
各大漏洞库的东西也可以加一些进去  
  
提权方面的也没有看到  
  
木马病毒免杀  
  
红队cs隐藏之类的  
  
供应链攻击  
  
Wi-Fi  
  
内鬼  
  
过期帐号  
测试账号  
  
那个深信服VPN 0day?  
  
  
恩  
  
  
安全设备就是安全厂商的一些设备漏洞  
  
  
奇安信  
天融信  
绿盟  
深信服  
启明星辰  
安恒  
.......  
  
  
比如华为防火墙的审计帐号很多人都不删除  
  
  
还有一些后门  
  
  
比如phpstudy  
宝塔/pma  
  
  
  
  
  
很多人都用同一个密码  
  
  
  
  
你有密码共用的地方写上去即可  
  
whovian 2021/9/21 10:32:53  
  
  
  
  
私人密码共用  
私人信息泄露  
社工私人  
私人电脑被拿下  
公司一些文档会被存储在私人电脑上  
  
  
私人电脑接入企业办公  
  
  
企业沦陷  
  
  
  
哪怕企业只有一个人中招,都可能给企业带来毁灭性的损失  
  
  
APT这样做  
其他的黑客也这样做  
  
  
  
  
红蓝对抗也有这样做的  
  
  
往员工邮箱发送带病毒的邮件  
  
  
员工的一些信息很好获取的  
  
  
反正不要有侥幸心理  
能想到的都应该去防御  
  
红蓝对抗表面上只是几星期  
  
  
有些人提前几个月就开始搜集这些信息了  
  
不然分数上不好看  
  
当当靠网站很多都是搞不下来的  
  
  
直接往员工邮箱，往公司门口撒U盘这种，我还是把它放到上边比较容易实施的那块。  
  
  
  
  
比赛的时候号称10秒钟攻破浏览器  
  
其实私下里搞了可能好几年  
  
  
  
CMS类型的漏洞也可以单独写一篇  
  
  
CMS有几百种  
可以写几百页  
  
我其实是把 CMS的这个写到框架那边去了。包括FCK EDITOR这种编辑器  
  
  
框架跟组件