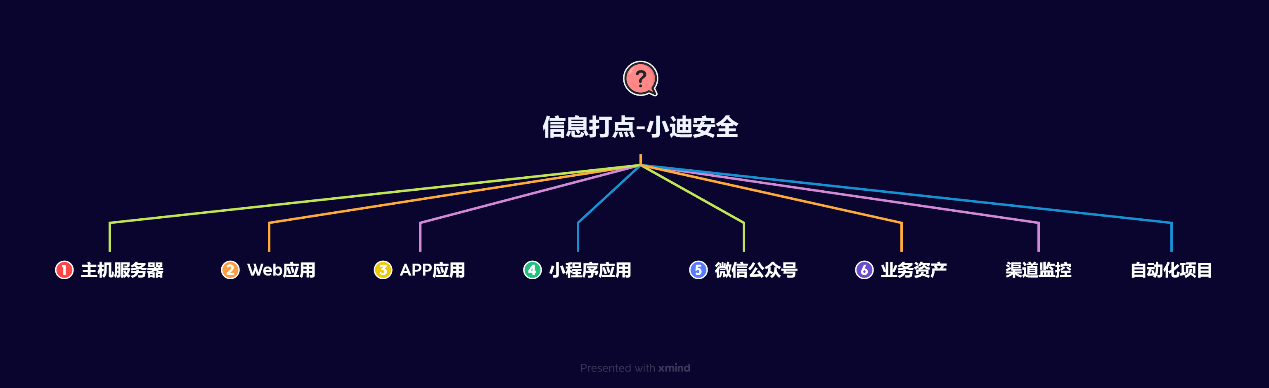
信息收集-Web应用&备案产权&Whois反查&域名枚举&DNS记录&证书特征&相似查询



#知识点：  
1、信息收集-服务器系统-操作系统&IP资产  
2、信息收集-服务器系统-端口扫描&服务定性  
---------------------------------------------------  
1、信息收集-Web应用-机构产权&域名相关性  
2、信息收集-Web应用-DNS&证书&枚举子域名  
  
#章节点：(待补充)  
#具体点：(待补充)

|  |  |  |
| --- | --- | --- |
| **标签** | **名称** | **地址** |
| 企业信息 | 天眼查 | <https://www.tianyancha.com/> |
| 企业信息 | 小蓝本 | <https://www.xiaolanben.com/> |
| 企业信息 | 爱企查 | <https://aiqicha.baidu.com/> |
| 企业信息 | 企查查 | <https://www.qcc.com/> |
| 企业信息 | 国外企查 | <https://opencorporates.com/> |
| 企业信息 | 启信宝 | <https://www.qixin.com/> |
| 备案信息 | 备案信息查询 | <http://www.beianx.cn/> |
| 备案信息 | 备案管理系统 | <https://beian.miit.gov.cn/> |
| 注册域名 | 域名注册查询 | <https://buy.cloud.tencent.com/domain> |
| IP反查 | IP反查域名 | <https://x.threatbook.cn/> |

|  |  |  |
| --- | --- | --- |
| **标签** | **名称** | **地址** |
| DNS数据 | dnsdumpster | <https://dnsdumpster.com/> |
| 证书查询 | CertificateSearch | <https://crt.sh/> |
| 网络空间 | FOFA | <https://fofa.info/> |
| 网络空间 | 全球鹰 | <http://hunter.qianxin.com/> |
| 网络空间 | 360 | [https://quake.360.cn/quake/](https://quake.360.cn/quake/#/index) |
| 威胁情报 | 微步在线 情报社区 | <https://x.threatbook.cn/> |
| 威胁情报 | 奇安信 威胁情报中心 | <https://ti.qianxin.com/> |
| 威胁情报 | 360 威胁情报中心 | <https://ti.360.cn/#/homepage> |
| 枚举解析 | 在线子域名查询 | <http://tools.bugscaner.com/subdomain/> |
| 枚举解析 | DNSGrep子域名查询 | <https://www.dnsgrep.cn/subdomain> |
| 枚举解析 | 工具强大的子域名收集器 | <https://github.com/shmilylty/OneForAll> |

|  |  |  |
| --- | --- | --- |
| **标签** | **名称** | **地址** |
| 网络空间 | 钟馗之眼 | [https://www.zoomeye.org/](https://www.zoomeye.org/?R1nG) |
| 网络空间 | 零零信安 | <https://0.zone/> |
| 网络空间 | Shodan | <https://www.shodan.io/> |
| 网络空间 | Censys | <https://censys.io/> |
| 网络空间 | ONYPHE | <https://www.onyphe.io/> |
| 网络空间 | FullHunt | <https://fullhunt.io/> |
| 网络空间 | Soall Search Engine | <https://soall.org/> |
| 网络空间 | Netlas | <https://app.netlas.io/responses/> |
| 网络空间 | Leakix | <https://leakix.net/> |
| 网络空间 | DorkSearch | <https://dorksearch.com/> |
| 威胁情报 | VirusTotal在线查杀平台 | <https://www.virustotal.com/gui/> |
| 威胁情报 | VenusEye 威胁情报中心 | <https://www.venuseye.com.cn/> |
| 威胁情报 | 绿盟科技 威胁情报云 | <https://ti.nsfocus.com/> |
| 威胁情报 | IBM 情报中心 | <https://exchange.xforce.ibmcloud.com/> |
| 威胁情报 | 天际友盟安全智能平台 | [https://redqueen.tj-un.com](https://redqueen.tj-un.com/IntelHome.html) |
| 威胁情报 | 华为安全中心平台 | [https://isecurity.huawei.com/sec](https://isecurity.huawei.com/sec/web/intelligencePortal.do) |
| 威胁情报 | 安恒威胁情报中心 | <https://ti.dbappsecurity.com.cn/> |
| 威胁情报 | AlienVault | <https://otx.alienvault.com/> |
| 威胁情报 | 深信服 | [https://sec.sangfor.com.cn/](https://sec.sangfor.com.cn/analysis-platform) |
| 威胁情报 | 丁爸情报分析师的工具箱 | <http://dingba.top/> |
| 威胁情报 | 听风者情报源 start.me | <https://start.me/p/X20Apn> |
| 威胁情报 | GreyNoise Visualizer | <https://viz.greynoise.io/> |
| 威胁情报 | URLhaus 数据库 | <https://urlhaus.abuse.ch/browse/> |
| 威胁情报 | Pithus | <https://beta.pithus.org/> |

演示案例：

* 应用服务器-操作系统&IP资产
* 应用服务器-端口扫描&角色定性
* Web应用-机构产权&域名相关性
* Web应用-子域名&DNS&证书&枚举

#操作系统  
1、Web大小写  
2、端口服务特征  
3、TTL值判断返回  
  
#IP资产  
归属地查询  
归属云厂商  
IP反查机构  
IP反查域名  
IP-C段查询  
这里可以转换成Web上，机构上，从而获取更多信息  
  
#端口资产  
1、网络资产引擎：直接使用网络测绘引擎(Fofa、Hunter、Quake、00信安等搜索IP；此类网络资产测绘引擎都是每隔一段时间会对全网的网络资产去做一个轮询，那可能每个引擎的轮询周期、扫描精准度都不同，故建议可使用不同的搜索引擎以获取更多资产。  
地址导航：https://dh.aabyss.cn/  
参考：https://mp.weixin.qq.com/s/FRgPQKJDj2xRCduwPfZrTw  
  
2、在线端口扫描：百度或google直接搜索在线端口扫描就会有一些网站，同理很多功能都可以直接搜索在线xxx；例如在线正则提取解析、在线编码转换等。  
  
3、本地离线工具：推荐使用Nmap、Masscan、Fscan、KScan，其中Nmap最为准确，但最慢；Masscan最快，误报相对更高。  
端口扫描：https://xz.aliyun.com/t/15753  
演示：Yakit Nmap TscanPlus FScan Tanggo等  
考虑：1、防火墙 2、内网环境  
可能出现案例：数据库端口开放，但进行端口扫描，发现数据库端口没有开放（排除防火墙）\*注意：扫描中选择扫描协议是绕过安全组防火墙设置的一种手法，具体成功需看出网入网配置  
  
#应用服务  
见上图端口协议对应服务应用  
  
#角色定性判定  
1、网站服务器  
2、数据库服务器  
3、邮件系统服务器  
4、文件存储服务器  
5、网络通信服务器  
6、安全系统服务器

主动信息收集：  
通过直接经过目标服务器网络流量的信息收集方式。  
  
被动信息收集：  
不与目标系统直接交互的情况下获取信息收集方式。  
  
域名：  
1、备案信息  
通过域名查备案信息，备案信息获取更多域名  
2、企业产权  
通过企业产权查询Web,APP,小程序等版权资产  
3、域名相关性  
Whois信息：例如域名所有人、域名注册商、邮箱等。  
通过域名注册接口获取后缀  
查询域名注册邮箱  
通过域名查询备案号  
通过备案号查询域名  
反查注册邮箱  
反查注册人  
通过注册人查询到的域名在查询邮箱  
通过上一步邮箱去查询域名  
查询以上获取出的域名的子域名  
  
子域名：  
在后续测试中，还要注意对子域名进行筛选整理，太多的垃圾子域名和没用的子域名，主要看你的收集的子域名方法决定。  
1、DNS数据  
以DNS解析历史记录查询域名资产  
2、证书查询  
以SSL证书解析查询域名资产  
3、网络空间  
多网络空间综合型获取的记录  
4、威胁情报  
各类接口的集成的记录  
5、枚举解析  
结果主要以字典决定  
https://github.com/knownsec/ksubdomain  
https://github.com/shmilylty/OneForAll  
6、JS提取子域名  
后续会讲到

涉及资源：[资源下载地址](https://docs.qq.com/doc/DQ3Z6RkNpaUtMcEFr)