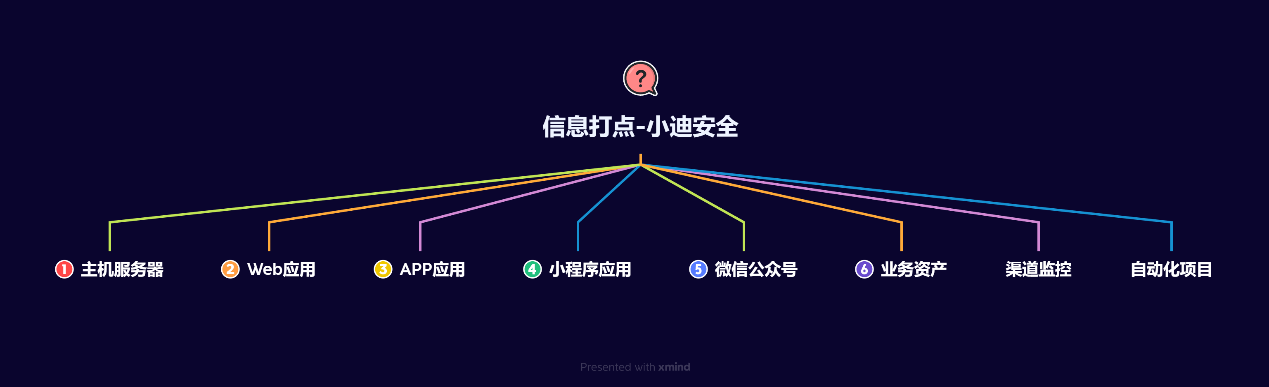
信息收集-Web应用&源码获取&闭源备份开发泄漏&WebPack打包&资源搜索&ICO定位



#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  
---------------------------------------------------  
1、信息收集-Web应用-架构分析&指纹识别  
2、信息收集-Web应用-架构分析&WAF&蜜罐  
3、信息收集-Web应用-架构分析&框架组件识别  
---------------------------------------------------  
1、信息收集-Web应用-源码获取-已知指纹&未知指纹  
2、信息收集-Web应用-源码获取-泄漏问题&发现指纹  
  
#章节点：(待补充)  
#具体点：(待补充)

|  |  |  |
| --- | --- | --- |
| **标签** | **名称** | **地址** |
| 指纹识别 | EHole\_magic | <https://github.com/lemonlove7/EHole_magic> |
| 指纹识别 | Wappalyzer | <https://github.com/AliasIO/wappalyzer> |
| 指纹识别 | TideFinger潮汐 | <http://finger.tidesec.net/> |
| 指纹识别 | 云悉指纹 | <https://www.yunsee.cn/> |
| 指纹识别 | hfinger | <https://github.com/HackAllSec/hfinger> |
| 指纹识别 | 数字观星Finger-P | <https://fp.shuziguanxing.com/#/> |
| 指纹识别 | CMSeek | <https://github.com/Tuhinshubhra/CMSeeK> |

演示案例：

* Web应用-架构分析-WAF&蜜罐识别
* Web应用-架构分析-框架组件指纹识别
* Web应用-源码获取-已知指纹&未知指纹
* Web应用-源码获取-泄漏问题&发现指纹

#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

#Web架构  
开源CMS：  
Discuz、WordPress、PageAdmin、蝉知等  
  
前端技术：  
HTML5、Jquery、Bootstrap、Vue、NodeJS等  
  
开发语言：  
PHP、JAVA、Ruby、Python、C#、JS、Go等  
  
框架组件：  
SpringMVC、Thinkphp、Yii、Tornado、Vue等  
  
Web服务器：  
Apache、Nginx、IIS、Lighttpd等  
  
应用服务器：  
Tomcat、Jboss、Weblogic、Websphere等  
  
数据库类型：  
端口扫描，组合判断，应用功能  
Mysql、SqlServer、Oracle、Redis、MongoDB等  
  
操作系统信息：  
Linux、Windows、Mac等  
  
应用服务信息：  
FTP、SSH、RDP、SMB、SMTP、LDAP、Rsync等  
  
CDN信息：  
帝联、Cloudflare、网宿、七牛云、阿里云等  
  
WAF信息：  
创宇盾、宝塔、ModSecurity、玄武盾、OpenRASP等。  
  
蜜罐信息：  
HFish、TeaPot、T-Pot、Glastopf等  
  
其他组件信息：  
FastJson、Shiro、Log4j、Solr、XStream等  
  
#指纹识别：  
1、平台：  
https://www.yunsee.cn/ http://finger.tidesec.net/  
https://fp.shuziguanxing.com/  
  
2、项目：  
https://github.com/AliasIO/wappalyzer  
https://github.com/HackAllSec/hfinger  
https://github.com/Tuhinshubhra/CMSeeK  
https://github.com/lemonlove7/EHole\_magic  
https://github.com/emo-crab/observer\_ward   
3、使用网络空间的ico识别  
借助目标的ic图标进行识别  
  
#WAF识别：  
拦截页面，identywaf项目内置  
https://github.com/stamparm/identYwaf  
https://github.com/EnableSecurity/wafw00f  
  
#蜜罐识别：  
1、项目识别：  
https://github.com/graynjo/Heimdallr  
https://github.com/360quake/quake\_rs  
quake.exe init apikey值  
quake.exe honeypot 目标  
2、人工识别：  
\*端口多而有规律性（针对多服务蜜罐）  
\*Web访问协议就下载（针对多服务蜜罐）  
\*设备指纹分析（见上图，针对蜜罐特征）  
  
#框架组件识别：  
后续会讲到更多识别方法及项目插件  
例子：  
FastJson：https://forum.butian.net/share/1679  
Shiro：https://mp.weixin.qq.com/s/j1nDnb0Ub5bk2-Tq5tt2pg

参考：  
https://www.secpulse.com/archives/124398.html  
https://mp.weixin.qq.com/s/QgLDdaefXlZtvlSiFQShZw  
https://mp.weixin.qq.com/s/zhjxW2mUEgq6dFAp3kBcgQ  
  
#源码泄漏原因：  
1、从源码本身的特性入口  
2、从管理员不好的习惯入口  
3、从管理员习惯的开发入口  
4、从管理员不好的配置入口  
5、从管理员不好的意识入口  
6、从管理员资源信息搜集入口  
源码泄漏大概集合：  
Webpack打包泄漏  
composer.json  
GitHub源码泄漏  
git源码泄露  
svn源码泄露  
网站备份压缩文件  
DS\_Store文件泄露  
hg源码泄漏  
SWP 文件泄露  
CVS泄露  
Bzr泄露  
WEB-INF/web.xml 泄露  
  
思路点：  
1、使用指纹识别平台获取到目标是什么名字的源码程序  
通过搜索引擎获取到源码  
  
2、使用指纹识别平台不能获取目标信息  
后端：借助svn git composer.json ds\_store 备份扫描等配置泄漏安全  
前端：webpack打包 谷歌插件获取源码  
如果没有这些问题 还想获取源码怎么办 见下面方法  
  
3、借助资源平台去搜索（github gitee oschina等源码）  
-特定文件  
-特征联系方式  
-github监控（ 除了源码，漏洞更新，工具更新等都有用处）  
目标使用的源码是开源还是闭源，是否公开  
  
#演示案例：  
1、已知指纹识别获取源码途径  
  
2、GIT泄漏-未知指纹识别获取源码途径  
3、SVN泄漏-未知指纹识别获取源码途径  
4、DS\_Store泄漏-未知指纹识别获取源码途径  
GIT：https://github.com/lijiejie/GitHack  
SVN：https://github.com/callmefeifei/SvnHack  
DS\_Store：https://github.com/lijiejie/ds\_store\_exp  
通用：https://github.com/0xHJK/dumpall  
  
5、WebPack打包-未知指纹识别获取源码途径  
https://github.com/NothingCw/SourceDetector-dist  
  
6、composer.json-未知指纹识别获取源码途径  
7、源码文件备份泄漏-未知指纹识别获取源码途径  
目录文件扫描工具获取存在，直接访问  
 8、Github资源搜索-未知指纹识别获取源码途径  
\*拓展：配合后期监控保证第一时间通知  
资源搜索语法：  
in:name test #仓库标题搜索含有关键字   
in:descripton test #仓库描述搜索含有关键字   
in:readme test #Readme文件搜素含有关键字   
stars:>3000 test #stars数量大于3000的搜索关键字   
stars:1000..3000 test #stars数量大于1000小于3000的搜索关键字 forks:>1000 test #forks数量大于1000的搜索关键字   
forks:1000..3000 test #forks数量大于1000小于3000的搜索关键字 size:>=5000 test #指定仓库大于5000k(5M)的搜索关键字 pushed:>2019-02-12 test #发布时间大于2019-02-12的搜索关键字 created:>2019-02-12 test #创建时间大于2019-02-12的搜索关键字 user:test #用户名搜素   
license:apache-2.0 test #明确仓库的 LICENSE 搜索关键字 language:java test #在java语言的代码中搜索关键字   
user:test in:name test #组合搜索,用户名test的标题含有test的  
关键字配合谷歌搜索：  
site:Github.com smtp   
site:Github.com smtp @qq.com   
site:Github.com smtp @126.com   
site:Github.com smtp @163.com   
site:Github.com smtp @sina.com.cn   
site:Github.com smtp password   
site:Github.com String password smtp  
  
9、另类目标源码获取  
https://www.huzhan.com/  
https://www.goofish.com/  
从目标转到寻找源码系统上，从源码系统上找应用目标  
  
#源码泄漏实战文章  
渗透测试实战---某资金盘信息收集(.idea目录泄露)  
https://mp.weixin.qq.com/s/7cSrDZci\_drE6wTGvQOOHw  
SRC挖掘-js.map泄露到接管云上域控  
https://mp.weixin.qq.com/s/QZsNjbTiaqC1qwzARVAiGQ

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