一、前言

在众测中，基本上SRC的漏洞收集范围有如下几种形式：

```
形式一：暂时仅限以下系统：www.xxx.com,其他域名不在此次测试范围内
形式二：只奖励与*.xxx.com相关的漏洞
形式三：无限制

形式一，基本被限定了范围
形式二，注重于子域名的收集
形式三，子域名及相关域名的收集
```

另外，随着企业内部业务的不断壮大，各种业务平台和管理系统越来越多，很多单位往往存在着“隐形资产”，这些“隐形资产”通常被管理员所遗忘，长时间无人维护，导致存在较多的已知漏洞。

在渗透测试中，我们需要尽可能多的去收集目标的信息，资产探测和信息收集，决定了你发现安全漏洞的几率有多大。如何最大化的去收集目标范围，尽可能的收集到子域名及相关域名的信息，这对我们进一步的渗透测试显得尤为重要。

在这里，通过介绍一些资产探测和信息收集的技巧，来收集渗透目标的信息。

假设我们只拿到了一个主域名。

二、资产探测

从主域名出发，我们首先需要考虑的是子域名，即*.xxx.com，接下来进行子域名搜集思路的梳理。

2.1 子域名收集

A、搜索引擎查询

```
Google、baidu、Bing等传统搜索引擎
site:baidu.com inurl:baidu.com
搜target.com|公司名字

网络空间安全搜索引擎
zoomeye(钟馗之眼)：https://www.zoomeye.org
shodan：https://www.shodan.io
Fofa：https://fofa.so
Censys：https://www.censys.io
Dnsdb搜索引擎：https://www.dnsdb.io

PS：可编写Python脚本批量查询、获取
```

B、在线查询接口

```
http://tool.chinaz.com/subdomain/
http://i.links.cn/subdomain/
http://subdomain.chaxun.la/
http://searchdns.netcraft.com/
https://www.virustotal.com/
https://censys.io/
https://x.threatbook.cn/ 微步在线
```

C、子域名暴力猜解

```
爆破工具：
Layer子域名挖掘机
wydomain：https://github.com/ring04h/wydomain
subDomainsBrute:https://github.com/lijiejie/
Sublist3r:https://github.com/aboul3la/Sublist3r
```

D、DNS查询/枚举

```
DNS查询：
host -t a domainName
host -t mx domainName

优点：非常直观，通过查询DNS服务器的A记录、CNAME等，可以准确得到相关信息，较全。
缺点：有很大的局限性，很多DNS是禁止查询的。
参考：https://www.cnblogs.com/xuanhun/p/3489038.html

域传送漏洞

DNS暴力破解：fierce
参考链接：http://blog.csdn.net/jeanphorn/article/details/44987549

Passive DNS
参考链接：http://www.freebuf.com/articles/network/103815.html
```

E、HTTPS证书

```
证书颁发机构(CA)必须将他们发布的每个SSL/TLS证书发布到公共日志中。SSL/TLS证书通常包含域名、子域名和电子邮件地址。因此SSL/TLS证书成为了攻击者的切入点。

SSL证书搜索引擎：
https://certdb.com/domain/github.com
https://crt.sh/?q=github.com
https://censys.io/

基于 HTTPS 证书的子域名收集小程序 ：GetDomainsBySSL.py
参考链接：http://www.freebuf.com/articles/network/140738.html
```

F、综合搜索

提莫：https://github.com/bit4woo/teemo
主要有三大模块：搜索引擎 第三方站点 枚举

利用全网IP扫描http端口 在访问IP的80或者8080端口的时候，可能会遇到配置了301跳转的，可以在header里获取域名信息。
全网扫描结果如下：https://scans.io/study/sonar.http

G、子域名筛选

当收集的子域名数量过大，手动筛选工作量太大，如何快速扫描，半自动的筛选出有效的可能存在漏洞的子域名。
参考链接：http://www.52bug.cn/%E9%BB%91%E5%AE%A2%E6%8A%80%E6%9C%AF/3413.html

2.2 相关域名收集：

A、旁站及c段收集

同IP网站及C段查询
IP反查域名

工具：御剑、K8
在线查询工具：
http://www.hackmall.cn/
http://www.webscan.cc/ 推荐
https://phpinfo.me/bing.php

将C段收集的相关IP，推测该单位所在的IP段，再针对IP段进行服务器端口扫描

B、端口扫描

对1-65535端口扫描，探测web服务端口

C、主站提取

通过编写爬虫，从主站页面（一般在主页）获取相关业务系统
思路是：通过访问主域名或者子域名，然后爬取页面上该域名的所有子域名，
然后循环访问获取到的子域名，然后再次循环，直到爬完为止

跨域策略文件 crossdomain.xml
如：https://www.baidu.com/crossdomain.xml

D、移动端

随着移动端的兴起，很多单位都有自己的移动APP、微信公众号、支付宝生活号等，这也是值得重点关注的点。

E、行业系统

```
同行业可能存在类似的系统，甚至于采用同一家厂商的系统，可互做对比
通用：办公OA、邮件系统、VPN等
医院：门户、预约系统、掌上医院、微信公众平台等
```

三、信息收集

主要是针对单个站点的信息收集技巧，主要围绕服务器IP、域名、网站。

3.1 服务器IP

A、绕过CDN查找网站真实ip

```
1、查询历史DNS记录：
查看 IP 与 域名绑定的历史记录，可能会存在使用 CDN 前的记录，相关查询网站有：
https://dnsdb.io/zh-cn/
https://x.threatbook.cn/
http://toolbar.netcraft.com/site_report?url=
http://viewdns.info/

2、xcdn
    https://github.com/3xp10it/xcdn

3、Zmap扫描全网
操作方法：http://bobao.360.cn/learning/detail/211.html

Tips：找到真实ip，绑定host ，是否可以打开目标网站，就是真实IP，对真实IP进行入侵测试，DDOS流量攻击，CC等等，实现无视CDN防御。
```

B、识别服务器及中间件类型

```
远程操作系统探测
用 NMAP 探测操作系统
```

C、端口及服务

```
Nmap  1-65535端口扫描，探测端口服务
```

D、查询IP所在位置

```
IP地址查询：
http://www.hao7188.com
http://www.882667.com
```

3.2 域名

A、搜索引擎

```
Google Hacking
Google Hacking查找，如site:baidu.com inurl:admin，使用类似语法，获取网站的敏感信息
```

B、whois信息/DNS解析

```
在whois查询中，获取注册人姓名和邮箱、电话信息，可以通过搜索引擎，社交网络，进一步挖掘出更多域名所有人的信息
DNS服务器
http://whois.chinaz.com
https://whois.aliyun.com
域名注册邮箱，可用于社工或是登录处的账号。
```

3.3 站点

A、robots.txt

```
网站通过Robots协议告诉搜索引擎哪些页面可以抓取，哪些页面不能抓取，可能存在一些敏感路径。
```

B、网站架构

```
网站语言、数据库，网站框架、组件框架历史漏洞
常用的网站架构如：LAMP/LNMP
PHP框架：ThinkPHP
```

C、目录结构/后台地址

```
常见的敏感目录以及文件扫描,这些对以后的突破都可能产生至关重要的作用。
收集的方式有爬虫采集，目录扫描
1）使用爬虫获取网站目录结构。如wvs爬虫功能获取网站目录结构。
2）使用目录猜解工具暴力猜解。如：御剑后台扫描工具、7kbscan-WebPathBrute
```

D、敏感文件信息泄露

```
备份文件、测试文件、Github泄露、SVN源码泄露
```

E、web 指纹

```
云悉在线WEB指纹CMS识别平台：http://www.yunsee.cn
```

F、安全防护

```
安全防护，云waf、硬件waf、主机防护软件、软waf
```

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。


Bypass