子域名信息搜集思路与技巧梳理

转载

FLy_鹏程万里 于 2018-06-28 23:25:49 发布 486 收藏

前言

本文适合Web安全爱好者，其中会提到8种思路，7个工具和还有1个小程序，看本文前需要了解相关的Web基础知识、子域名相关概念和Python 程序的基础知识。

感谢我的好友**龙哥**的技巧大放送以及**Oritz**分享的小程序~

首先我们引用一句名言作为开篇：

> 在渗透测试中，信息搜集能力的差距，不明显，也最明显。

这句话是龙哥说的，而在技术分享上，我们觉得授之以鱼之前，更重要的是授之以渔。因此本篇文章首先进行子域名搜集思路的梳理，抛砖引玉，然后介绍一下常用的工具，最后分享一个基于 HTTPS 证书的子域名查询小工具。

思路梳理及操作图示

1、Web子域名猜测与访问尝试

最简单的一种方法，对于 Web 子域名来说，猜测一些可能的子域名，然后浏览器访问下看是否存在。

2、搜索引擎查询

比如 site:163.com

3、查询DNS的一些解析记录

如查询 MX、CNAME 记录等

比如用 nslookup 命令

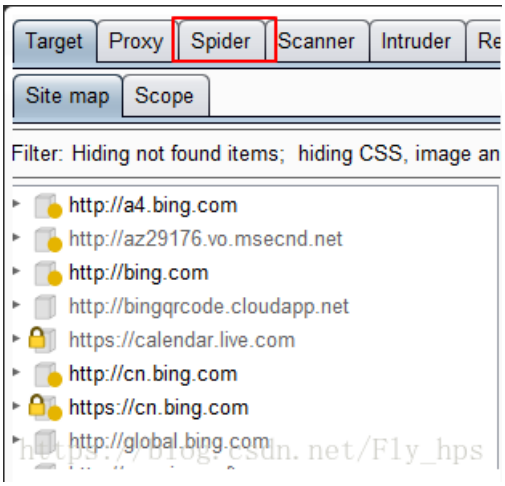
```
nslookup -qt=any bing.com
```

还有一种基于DNS查询的暴力破解，举个栗子，比如用 nslookup 命令挨个查询猜测的子域名，看能否查询到结果。

4、爬虫爬取页面提取子域名

可以利用爬虫从页面源代码中提取子域名

以 burp 的爬虫为例：

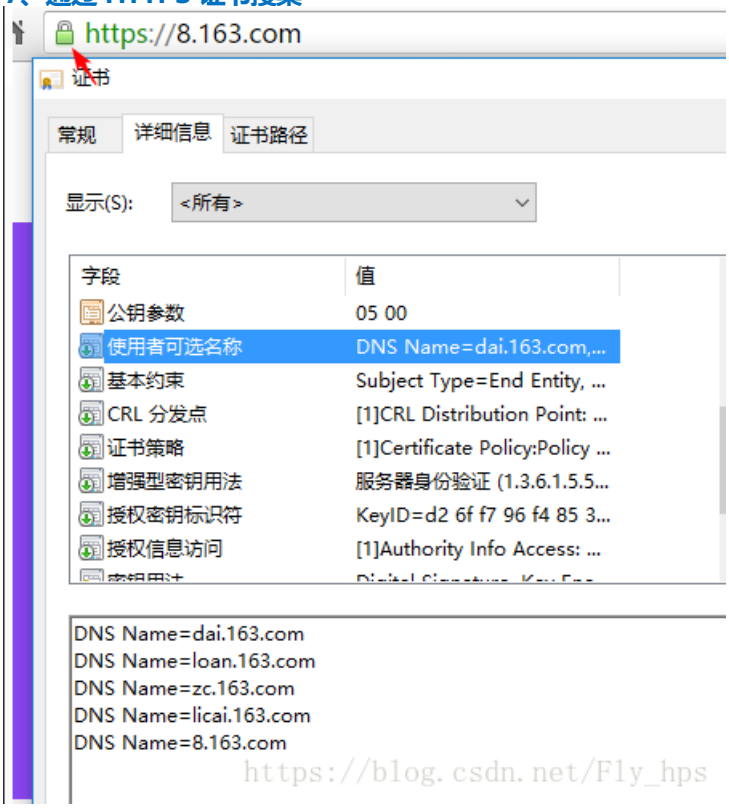


5、crossdomain.xml 文件

6、通过 IP 反查（类似于旁站查询）

至于 IP 如何获取，也会有一些玩法，有机会咱们再梳理。

7、通过 HTTPS 证书搜集



8、一些漏洞的利用

如： DNS 域传送漏洞

常用工具梳理

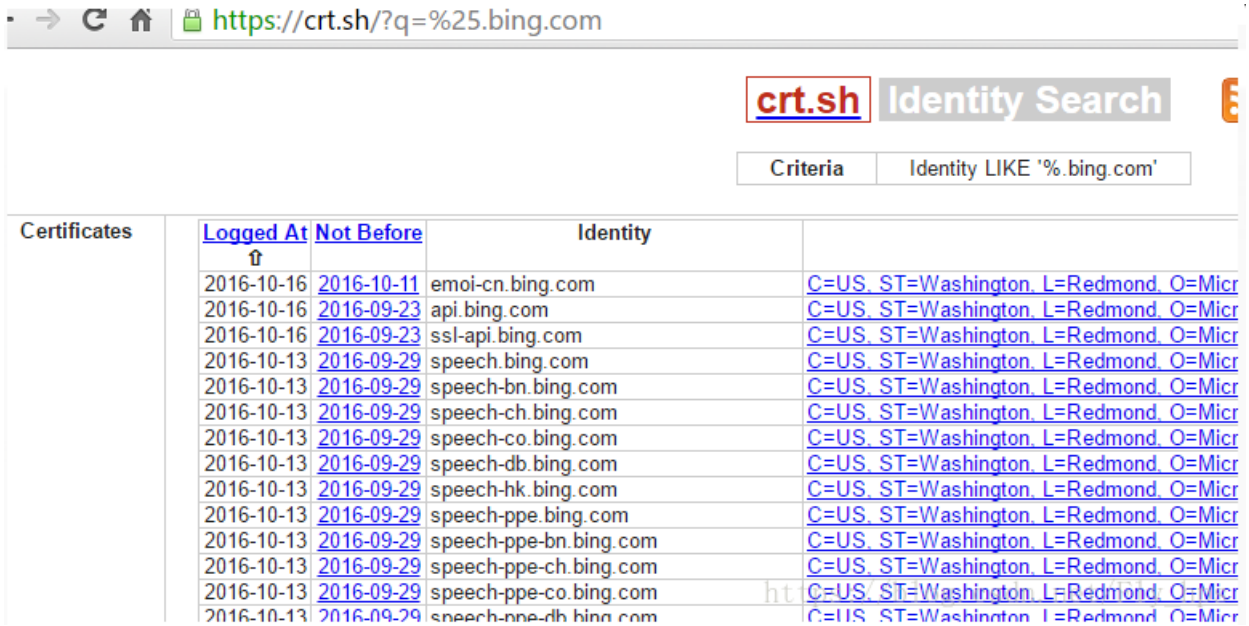
1、在线工具

有很多子域名的查询站点，可以搜索“子域名查询”寻找，如：

1）http://i.links.cn/subdomain/ 可查询二级、三级等子域名

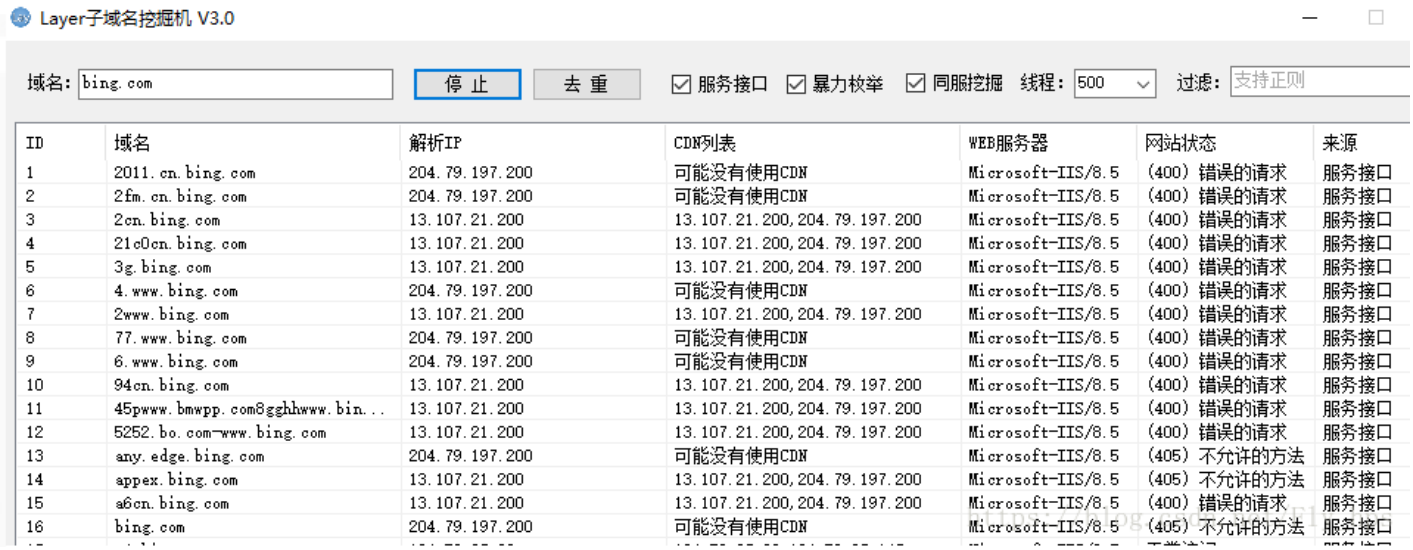
2）http://dns.aizhan.com/ 查询同 IP 绑定了哪些域名

3）https://crt.sh/ 根据 HTTPS 证书查询子域名



2、本地工具

1）Layer 子域名挖掘机



2）wydomain

猪猪侠：https://github.com/ring04h/wydomain

wydomain

目标系统信息收集组件，完全模块化，脚本均可拆可并、可合可分的使用！

运行流程

- 利用FOFA插件获取兄弟域名，并透视获取到的子域名相关二级域名、IP信息
- 检查域名和兄弟域名是否存在域传送漏洞,存在就遍历zone记录，将结果集推到wydomians数据组
- 获取可以获取的公开信息 MX、DNS、SOA记录
- 子域名字典暴力穷举域名(60000条字典[domain_default.csv])
- 利用第三方API查询子域名(links、alexa、bing、google、sitedossier、netcraft)
- 逐个域名处理TXT记录, 加入总集合
- 解析获取到的所有子域名，生成IP列表集合，截取成RFC地址C段标准(42.42.42.0/24)
- 利用bing.com、aizhan.com的接口，查询所有C段旁站的绑定情况
- 生成数据可视化报告
- 返回wydomains数据结果

3）subDomainsBrute

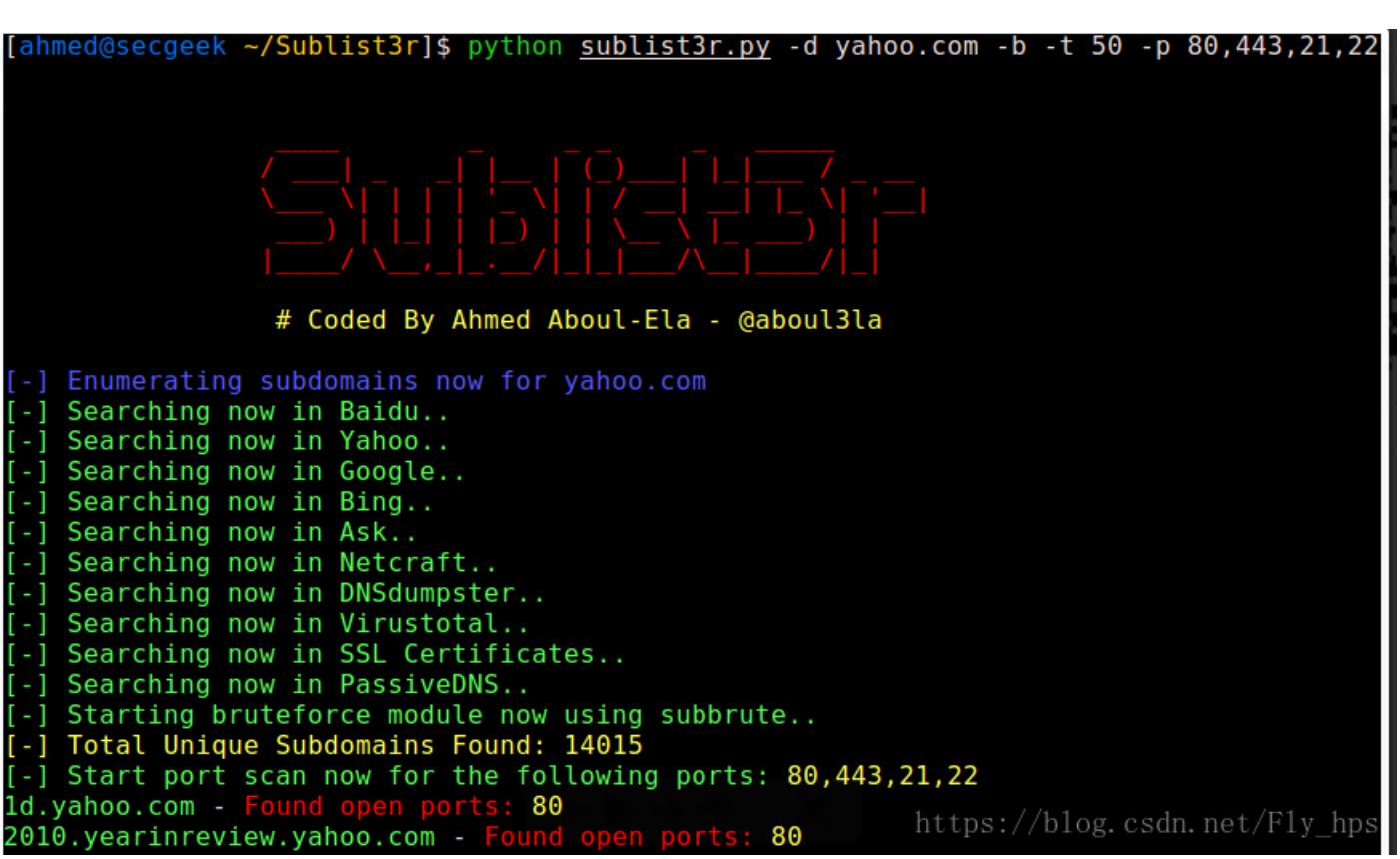
lijiejie:https://github.com/lijiejie/subDomainsBrute

Improvements

- 用小字典递归地发现三级域名，四级域名、五级域名等不容易被探测到的域名
- 字典较为丰富，小字典就包括1万5千条，大字典多达6万3千条
- 默认使用114DNS、百度DNS、阿里DNS这几个快速又可靠的Public DNS查询，可修改配置文件添加DNS服务器
- 自动去重泛解析的域名，当前规则： 超过2个域名指向同一IP，则此后发现的其他指向该IP的域名将被丢弃
- 速度尚可，在我的PC上，每秒稳定扫描约3百个域名（30个线程）

4）Sublist3r

aboul3la: https://github.com/aboul3la/Sublist3r



小程序分享

最后分享下团队小伙伴 Oritz 写的基于 HTTPS 证书的子域名收集练习小程序 “GetDomainsBySSL.py” ，程序异常处理之类的还没完善，感兴趣的小伙伴可以当做例子继续开发哦。

下载链接：Youdao

程序原理：集成了 crt.sh 和 Google 的查询接口，以及调用 OpenSSL 去解析 HTTPS 证书的信息（需要说明的是，Google 的查询接口可能需要代理访问，而 OpenSSL 模块在 Linux 下通常自带）。

程序依赖的模块：

> 1）lxml：https://pypi.python.org/pypi/lxml/2.3/
>
> 2）OpenSSL

Windows下运行（没有OpenSSL的情况运行）：

```
>python GetDomainsBySSL_161018.py outlook.com
[-] Get Domains from OpenSSL ...
[!] You have no OpenSSL or there is no HTTPS domain for outlook.com.
[-] Get Domains from crt.sh ...
[+] Number of Domains: 533
set(['pod71302.outlook.com', '064-1-d.outlook.com', 'safelinks.protection.outlook.com', 'pod51115ip
54-1-d.outlook.com', 'pod51152.outlook.com', 'pod51187psh.outlook.com', 'rms-055-2-d.prod.outlook.c
look.com', 'pod72029ip.outlook.com', 'pod72032ip.outlook.com', 'pod71132.outlook.com', 'rms-024-2-d
od71266-pri.outlook.com', 'pod51077ip.outlook.com', 'pod51114.outlook.com', 'pod71106.outlook.com'
m', 'pod71086-pri.outlook.com', 'pod51092.outlook.com', 'pod71099.outlook.com', 'pod71101.outlook.
d.outlook.com', 'support.outlook.com', '029-1-d.prod.outlook.com', 'rms-048-4-d.prod.outlook.com',
.com', 'pod51144.outlook.com', 'pod51121.outlook.com', 'pod71106-pri.outlook.com', 'pod71002.outlo
look.com', 'pod72030.outlook.com', 'pod51077.outlook.com', 'pod71027.outlook.com', '066-3-d.prod.o
ion.outlook.com', 'pod51142.outlook.com', 'pod71142-pri.outlook.com', 'pod51113psh.outlook.com', 'r
', '064-2-d.prod.outlook.com', 'pod51110-pri.outlook.com', 'pod71046.outlook.com', 'pod71038.outlo
.outlook.com', 'pod71109-pri.outlook.com', 'prdtrs01.prod.outlook.com', 'pod71112-pri.outlook.com'
.com', 'pod71054.outlook.com', 'rms-063-2-d.prod.outlook.com', 'pod51172psh.outlook.com', '046-2-d
d.prod.outlook.com', 'rms-048-7-d.prod.outlook.com', 'pod51112.outlook.com', 'pod51106.outlook.com
k.com', '062-2-d.prod.outlook.com', 'pod51120-pri.outlook.com', 'pod51096.outlook.com', 'pod51154-
d51084ip.outlook.com', 'pod71115-pri.outlook.com', 'pod71138.outlook.com', '062-1-d.prod.outlook.co
```

Linux下运行（kali自带了OpenSSL模块）：

```
lic# python GetDomainsBySSL.py  outlook.com
[-] Get Domains from OpenSSL ...
[+] Number of Domains: 8
set(['attachment.outlook.office.net', 'internal.outlook.com', 'outlook.of
m', 'live.com', 'office365.com', 'outlook.office365.com', 'attachment.out
ficeppe.net', 'office.com'])
[-] Get Domains from crt.sh ...
[+] Number of Domains: 533
set(['pod71302.outlook.com', '064-1-d.outlook.com', 'safelinks.protection
k.com', 'pod51115ip.outlook.com', 'rms-054-1-d.outlook.com', 'pod51152.ou
om', 'pod51187psh.outlook.com', 'rms-055-2-d.prod.outlook.com', 'pod51155
look.com', 'pod72029ip.outlook.com', 'pod72032ip.outlook.com', 'pod71132.
.com', 'rms-024-2-d.prod.outlook.com', 'pod71266-pri.outlook.com', 'pod51
```

好了，时间过得真快，又到了说再见的时候。今天的小分享就到这里，一句话概括就是8 种思路，7 个工具，还有 1个小程序，欢迎交流讨论哦~