【2022HW-蓝队】子域名收集常用工具总结（Layer、subDomainsBrute、sublist3r、dnsenum）

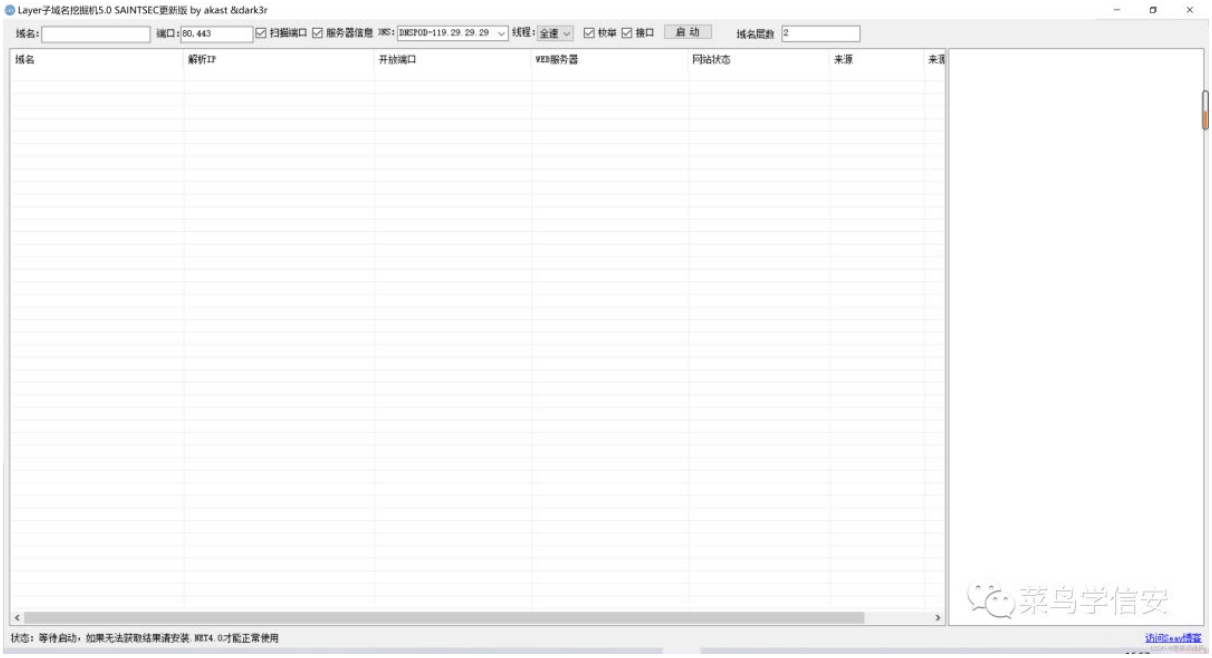
墨痕诉清风 Hacking黑白红 2022-06-16 09:00 Posted on 安徽

说明

子域名是某个主域的二级域名或者多级域名，在防御措施严密情况下无法直接拿下主域，那么就可以采用迂回战术拿下子域名，然后无限靠近主域。例如：www.xxxxx.com主域不存在漏洞，并且防护措施严密，而二级域名 edu.xxxxx.com存在漏洞，并且防护措施松散，那么就可以采用迂回战术拿下子域名，然后逐步靠近主域。

Layer子域名挖掘机

Layer子域名挖掘机使用方法简单，在域名对话框中直接输入域名就可以进行扫描，它的显示界面比较细致，有域名、解析IP、CDN列表、WEB服务器和网站状态

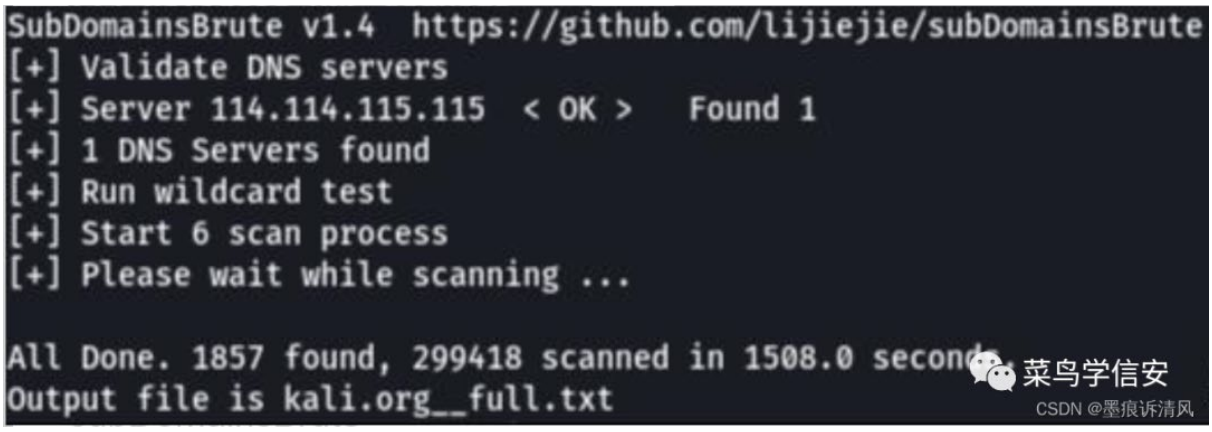


subDomainsBrute

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

subDomainsBrute的特点是可以用小字典递归地发现三级域名、四级域名，甚至五级域名等不容易被探测到的域名

使用方法：python3 subDomainsBrute.py --full xxx.com



sublist3r

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

Sublist3r也是一个比较常用的工具，它能列举多种资源，如在Google、Yahoo、Bing、Baidu和Ask等搜索引擎中可查到的子域名，还可以列出Netcraft、VirusTotal、ThreatCrowd、DNSdumpster和Reverse DNS查到的子域名

使用方法：python sublist3r.py -d xxx.com

dnsenum

https://github.com/fwaeytens/dnsenum/

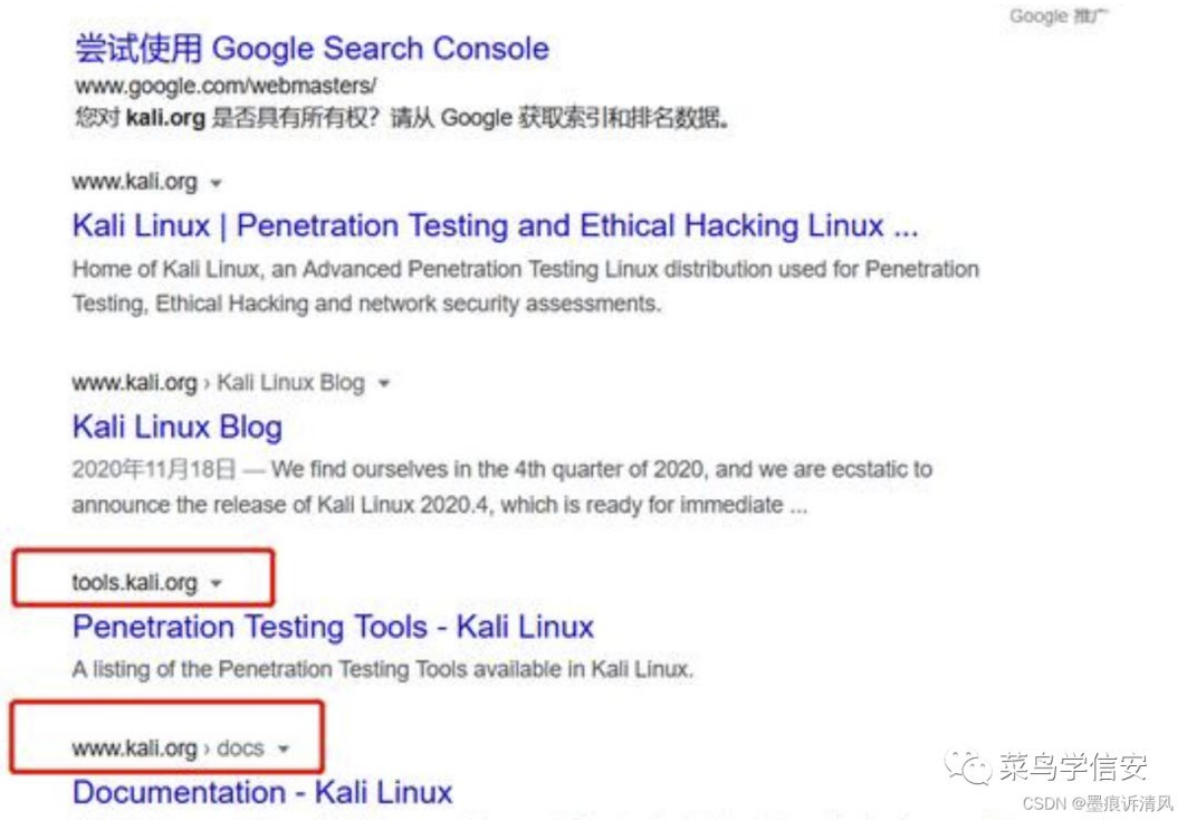
dnsenum的目的是尽可能收集一个域的信息，它能够通过谷歌或者字典文件猜测可能存在的域名，并对一个网段进行反向查询。它不仅可以查询网站的主机地址信息、域名服务器和邮件交换记录，还可以在域名服务器上执行axfr请求，然后通过谷歌脚本得到扩展域名信息，提取子域名并查询，最后计算C类地址并执行whois查询，执行反向查询，把地址段写入文件

使用方法：dnsenum xxx.com

```
kali@kali:~$ dnsenum kali.org
dnsenum VERSION:1.2.6

-----   kali.org   -----


Host's addresses:
__________________

kali.org.                            5        IN    A        192.124.249.10


Name Servers:
______________

ns-10-c.gandi.net.                   5        IN    A        217.70.187.11
ns-150-a.gandi.net.                  5        IN    A        173.246.100.151
ns-88-b.gandi.net.                   5        IN    A        213.167.230.89


Mail (MX) Servers:
___________________

alt1.aspmx.l.google.com.             5        IN    A        74.125.137.26
alt4.ASPMX.l.google.com.             5        IN    A        173.194.209.27
alt2.aspmx.l.google.com.             5        IN    A        64.233.180.26
aspmx.l.google.com.                  5        IN    A        108.177.125.26
alt3.ASPMX.l.google.com.             5        IN    A        209.85.147.27


Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for kali.org on ns-10-c.gandi.net ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for kali.org on ns-150-a.gandi.net ...
AXFR record query failed: NOTAUTH
```


Google Hacking搜索子域名

使用方法：site:kali.org



证书透明度公开日志枚举

证书透明度(Certificate Transparency，CT)是证书授权机构(CA)的一个项目，证书授权机构会将每个SSL/TLS证书发布到公共日志中。一个SSL/TLS证书通常包含域名、子域名和邮件地址，这些也经常成为攻击者非常希望获得的有用信息。查找某个域名所属证书的最简单的方法就是使用搜索引擎搜索一些公开的CT日志

https://crt.sh/
https://censys.io/

子域名在线枚举

https://phpinfo.me/domain/
https://chaziyu.com/
https://hackertarget.com/find-dns-host-records/
https://d.chinacycc.com/
https://www.t1h2ua.cn/tools/
https://dnsdumpster.com/
http://z.zcjun.com/
http://tool.chinaz.com/subdomain/

作者：墨痕诉清风
原文链接：https://blog.csdn.net/u012206617/article/details/123050983

END

【2022HW系列】|10-一次某次攻防演练种的分析溯源
【2022HVV系列】|9-红蓝对抗-红队打点的那些事
【2022HVV系列】|8-应急响应之入侵排查
【2022HVV系列】|7-Windows主机入侵痕迹排查办法
【2022HVV系列】|6-记一次hw中的上线骚姿势（异速联+用友U8）
【2022HVV系列】|5-记一次溯源过程
【2022HVV系列】|4-红蓝对抗 | 红队打点的那些事
【2022HVV系列】|3-服务器入侵排查
【2022HVV系列】| 2-应急响应常用工具