


信息收集篇——子域名的探测

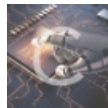
转载

小白渣  于 2019-11-28 21:01:55 发布  1826  收藏 5

分类专栏: [子域名探测](#) 文章标签: [渗透篇](#)

原文链接: https://blog.csdn.net/chest_/article/details/102605357

版权



[子域名探测](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

一. 实验目的

信息收集对于渗透测试前期来说是非常重要的,因为只有掌握了目标网站或目标主机足够多的信息之后,才能更好地对其进行漏洞检测,当我们要对一个目标进行渗透时,我们往往需要去尽可能的挖掘目标可能存在的攻击面。就拿一个域名来说,当主站防御的比较死的时候,通常就会考虑其子站。因为相对主站而言,子站的安全性做的可能不那么全面,而且dns是目前最主要的服务信息暴露来源,总的来说子域名探测是我们在信息集中重要的一环,帮助我们扩大渗透测试的范围以及开阔我们视野,所以我们有必要对dns进行详细的子域名探测分析

二. 实验原理

通过收集一个域的信息,能够通过谷歌或者字典文件猜测可能存在的域名,以及对一个网段进行反向查询。它可以查询网站的主机地址信息、域名服务器,由此得到查询出子域名的效果

三. 实验环境

谷歌浏览器

Kali渗透测试平台

网络环境: nat模式

四. 实验过程

一、整站分析

1.检测是否为cdn网站

首先,我们要判断该域名是否存在CDN的情况,cmd输入nslookup www.baidu.com检测百度是否使用了cdn

```
C:\Users\see you>nslookup www.baidu.com
服务器:  cache1-ja.bjtelecom.net
Address:  219.141.140.10

非权威应答:
名称:     www.a.shifen.com
Addresses: 220.181.38.149
           220.181.38.150
Aliases:  www.baidu.com
```

查询出的ip数量大于一个的,说明该ip地址不是真实的服务器地址

2.判断服务器类型

先说说ttl,TTL的作用是限制IP数据包在计算机网络中的存在的时间。TTL的最大值是255,TTL的一个推荐值是64。每过一个路由设备 TTL-1,所以到了本机后得到的TTL值肯定比目标的默认值小

通过ping来探测判断是服务器是Linux还是Windows,Windows的TTL值都是一般是128,Linux则是64。所以大于100的肯定是Windows,而几十的肯定是Linux。

```
C:\Users\see you>ping www.baidu.com

正在 Ping www.a.shifen.com [220.181.38.149] 具有 32 字节的数据:
来自 220.181.38.149 的回复: 字节=32 时间=4ms TTL=50
来自 220.181.38.149 的回复: 字节=32 时间=4ms TTL=50
来自 220.181.38.149 的回复: 字节=32 时间=4ms TTL=50
来自 220.181.38.149 的回复: 字节=32 时间=4ms TTL=50

220.181.38.149 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 4ms, 最长 = 4ms, 平均 = 4ms
```

如果要判断目标网站服务器的具体的版本的话,可以采用 nmap 进行扫描,-O 和 -A 参数都能扫描出来,这里采用-O参数 -o是列出操作系统版本

```
rtt min/avg/max/mdev = 6.265/6.702/7.196/0.387 ms
root@kali:~# nmap -O 220.181.38.150
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-20 19:48 CST
Nmap scan report for 220.181.38.150
Host is up (0.13s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP
Running: Actiontec embedded, Linux
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel
OS details: Actiontec MI424WR-GEN3I WAP

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 64.10 seconds
```

可以清楚的看出,这个服务器的操作系统为linux,具体信息如上

3. 查看web服务器的类型

在Kali终端通过命令whatweb www.baidu.com可以看到该服务器为阿帕奇

```
Server: Apache
Set-Cookie: BAIDUID=566D101456F81EE8ABEE49D19E60F600:FG=1; expires=Wed, 19-Aug-20 11:57:31 GMT; max-age=31536000; path=/; domain=.baidu.com; version=1
Vary: Accept-Encoding,User-Agent
Connection: close

root@kali:~# whatweb www.baidu.com
http://www.baidu.com [200 OK] Cookies[BAIDUID, BDSVRTM, BD_HOME, BIDUPSID, H_PS_PSSID, PSTM, delPer], Country[CHINA][CN], Email[baidu_resultlogo2.png], HTML5, HTTPServer[BWS/1.1], IP[220.181.38.149], JQuery, Meta-Refresh-Redirect[/baidu.html?from=script], OpenSearch[/content-search.xml], Script[text/javascript], Title[百度一下,你就知道], UncommonHeaders[bdpagetype,bdqid,xy_all], X-UA-Compatible[IE=Edge,IE=Edge,chrome=1]
http://www.baidu.com/baidu.html?from=script [200 OK] Apache, Cookies[BAIDUID], Country[CHINA][CN], HTML5, HTTPServer[Apache], IP[220.181.38.149], Script, Title[百度一下,你就知道], X-UA-Compatible[IE=Edge]

root@kali:~#
```

分析完毕后，我们就可以进行下一步的子域名探测了

二.子域名探测

一.爆破子域名

搜集完以上信息，我们就可以暴力破解目标域中的子域，一般用dnsenum这个工具来配合字典爆破子域名
终端输入命令: dnsenum -f /usr/share/dnsenum/dns.txt baidu.com

这次用的字典是Kali自带的字典，如果觉得威力不够，爆破失败可以自行去匹配别的字典

```
x86_64-w64-Injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? (Y/N)
[15:57:55] [INFO] testing 'MySQL UNION query (79) - 1 to 20 columns'
[15:57:58] [INFO] testing 'MySQL UNION query (79) - 21 to 40 columns'
[15:58:02] [INFO] testing 'MySQL UNION query (79) - 41 to 60 columns'
[15:58:07] [INFO] testing 'MySQL UNION query (79) - 61 to 80 columns'
[15:58:09] [INFO] testing 'MySQL UNION query (79) - 81 to 100 columns'
[15:58:11] [INFO] checking if the injection point on GET parameter 'id' is a false positive

[16:02:55] [ERROR] user quit

[*] ending @ 16:02:55 2019-08-20/

root@kali:~# dnsenum -f /usr/share/dnsenum/dns.txt baidu.com
Smartmatch is experimental at /usr/bin/dnsenum line 690.
Smartmatch is experimental at /usr/bin/dnsenum line 690.
dnsenum VERSION:1.2.4

----- baidu.com -----

Host's addresses:
-----
baidu.com.          5      IN      A       39.156.69.79
baidu.com.          5      IN      A       220.181.38.148

Name Servers:
-----
dns.baidu.com.      5      IN      A       202.108.22.220
ns3.baidu.com.      5      IN      A       112.80.248.64
ns2.baidu.com.      5      IN      A       220.181.33.31
ns4.baidu.com.      5      IN      A       14.215.178.80
ns7.baidu.com.      5      IN      A       180.76.76.92

Mail (Mx) Servers:
-----
-----
https://blog.csdn.net/chest_
```

爆破后的子域名

```
w64-Brute forcing with /usr/share/dnsenum/dns.txt:
11.baidu.com.      5      IN      CNAME   jpaasmatrix.e.shifen.com.
jpaasmatrix.e.shifen.com.  5      IN      A       220.181.57.55
a.baidu.com.      5      IN      CNAME   asp.e.shifen.com.
asp.e.shifen.com.  5      IN      A       220.181.44.96
abc.baidu.com.    5      IN      CNAME   www.a.shifen.com.
www.a.shifen.com.  5      IN      A       220.181.38.150
www.a.shifen.com.  5      IN      A       220.181.38.149
access.baidu.com.  5      IN      A       18.94.49.39
act.baidu.com.    5      IN      CNAME   eopa.n.shifen.com.
eopa.n.shifen.com.  5      IN      A       220.181.33.6
sys.admin.baidu.com.  5      IN      A       10.26.109.19
ads.baidu.com.    5      IN      A       10.42.4.225
usr.air.baidu.com.  5      IN      CNAME   szjjh-bvc-am1.szjjh01.baidu.com.
ap.baidu.com.     5      IN      CNAME   apbr.n.shifen.com.
apbr.n.shifen.com.  5      IN      A       180.149.132.182
arp.baidu.com.    5      IN      A       180.149.144.40
atlantic.baidu.com.  5      IN      A       10.26.5.60
atlantic.baidu.com.  5      IN      A       10.50.14.165
avatar.baidu.com.  5      IN      A       10.26.137.29
backup.baidu.com.  5      IN      A       10.149.145.28
bc.baidu.com.     5      IN      A       10.23.250.192
bce.baidu.com.    5      IN      A       220.181.33.180
bce.baidu.com.    5      IN      A       61.135.185.216
bce.baidu.com.    5      IN      A       39.156.66.242
bcss.baidu.com.   5      IN      A       183.232.232.58
bcss.baidu.com.   5      IN      A       153.37.235.60
bcss.baidu.com.   5      IN      A       180.101.49.157
beta.baidu.com.   5      IN      CNAME   beta.n.shifen.com.
beta.n.shifen.com.  5      IN      A       111.206.37.130
br.baidu.com.     5      IN      CNAME   search-br.wshifen.com.
search-br.wshifen.com.  5      IN      A       123.125.114.144
bugs.baidu.com.   5      IN      CNAME   fankui.icafe.baidu.com.
fankui.icafe.baidu.com.  5      IN      A       10.42.4.177
cap.baidu.com.    5      IN      A       180.97.184.99
cap.baidu.com.    5      IN      A       61.135.185.242
https://blog.csdn.net/chest_
```

服务器的c段网络

当然也可用其它的子域名爆破工具或者谷歌语法来检索主站下的子域名

如inurl去检索含有baidu.com的URL域名

The screenshot shows a Baidu search result for the query 'inurl:baidu.com'. The search bar at the top contains the query. The results are listed on the left side of the page, with several items highlighted by red boxes and a red arrow pointing to the search bar. The highlighted items are:

- 百度一下,你就知道**: 有事搜一搜 没事看一看 把百度设为首页关于百度 about baidu 百度推广 ©2019 Baidu 使用百度前必读 意见反馈 京icp证030173号 京公网安备11000002000001号 ... [lwww.baidu.com/](#) - 百度快照
- 登录**: 用户登录 账号类型 客户管理系统 用户名 密码 验证码 换一张 总部用户直接点此进入 对于新声系统有任何问题或建议,请给我们发信 ©2019 Baidu [huisheng.baidu.com/](#) - 百度快照
- 百度客户管理系统**: 收藏我们 12345登录 换一张安全控件常见问题 忘记密码对百度客户管理系统有任何意见和建议,请给我们发信 ... [icrm.baidu.com/](#) - 百度快照
- 登录百度帐号**: [lc.baidu.com/](#) - 由于该网站的robots.txt文件存在限制指令(限制搜索引擎抓取),系统无法提供该页面的内容描述 - 了解详情
- 百度推广**: 移动统计 转化与监控工具 爱番番 智能获客引擎 百度推广APP 推广辅助工具 ©2019 Baidu 使用百度前必读 百度首页 国家药监局(京)-经营性-2007-0007 ... [https://feedgd.baidu.com/](#) - 百度快照
- 百度推广-登录**: 百度推广 | 登录换一张 登录 ... [fep.baidu.com/](#) - 百度快照 - 7824条评价
- 百度贴吧**: [baidu.com官方吧_百度贴吧](#)
百度粉丝的专属聚集地
关注用户: 467万+

On the right side of the page, there is a '搜索热点' (Search Hotspots) section with a list of trending topics and their search volumes:

排名	搜索热点	热度
1	巩俐中国女排路透	752万
2	王丽坤否认结婚	694万
3	康辉又怒美国了	662万
4	地震预警覆盖四川	619万
5	雪莉今日出嫁	604万
6	梅西6夺欧洲金靴	489万
7	金秀贤新剧	434万
8	网曝那英准备离婚	367万
9	马云获终身成就奖	331万
10	南开大学灯光秀	329万

At the bottom right of the page, there is a URL: <https://blog.csdn.net/chesu>