Dnsmap

dnsmap最初是在2006年发布的，它的灵感来自于虚构的故事“小偷没有人看到”由保罗克雷格，可以找到在《Stealing the Network - How to 0wn the Box》一书中

dnsmap主要是供测试人员在测试期间使用基础设施安全评估的收集/列举阶段。在枚举阶段，安全顾问通常会发现目标公司的IP网块、域名、电话号码等...子域强制蛮力是应该在枚举阶段，因为它在其他域枚举时特别有用区域转移之类的技术不起作用(我很少看到区域转移顺便说一下，现在是“公开”允许的)。

如果你对研究隐秘的计算机入侵技术感兴趣，我建议你阅读这篇精彩(有趣)的章节，你可以从中找到*免费*在网上:

http://www.ethicalhacker.net/content/view/45/2/

我很高兴地告诉大家，dnsmap已经包括在回溯2、3和4中，并且已经被包括进去了
已获社会各界审阅:

http://backtrack.offensive-security.com/index.php?title=Tools
http://www.networkworld.com/community/node/57543
http://forums.remote-exploit.org/tutorials-guides/12746-dnsmap-tutorial.html
http://www.linuxhaxor.net/2007/07/14/backtrack-2-information-gathering-all-dnsmap/
http://www.darknet.org.uk/2009/03/dnsmap-022-released-subdomain-bruteforcing-tool/

—— *Felix Richter makefu*

一，帮助手册

dnsmap 0.35 - DNS网络映射器

用法:dnsmap <目标域>[选项]

选项:

- w < wordlist-file >
- r < regular-results-file >
- c < csv-results-file >
- d < delay-millisecs >

-i (如果获得误报，这很有用)

例如:

dnsmap example.com

dnsmap example.com -w yourwordlist.txt -r /tmp/domainbf_results.txt

dnsmap example.com -r /tmp/ - d3000

dnsmap example.com -r ./domainbf_results.txt

dnsmap 0.35 - DNS Network Mapper

usage: dnsmap [options]

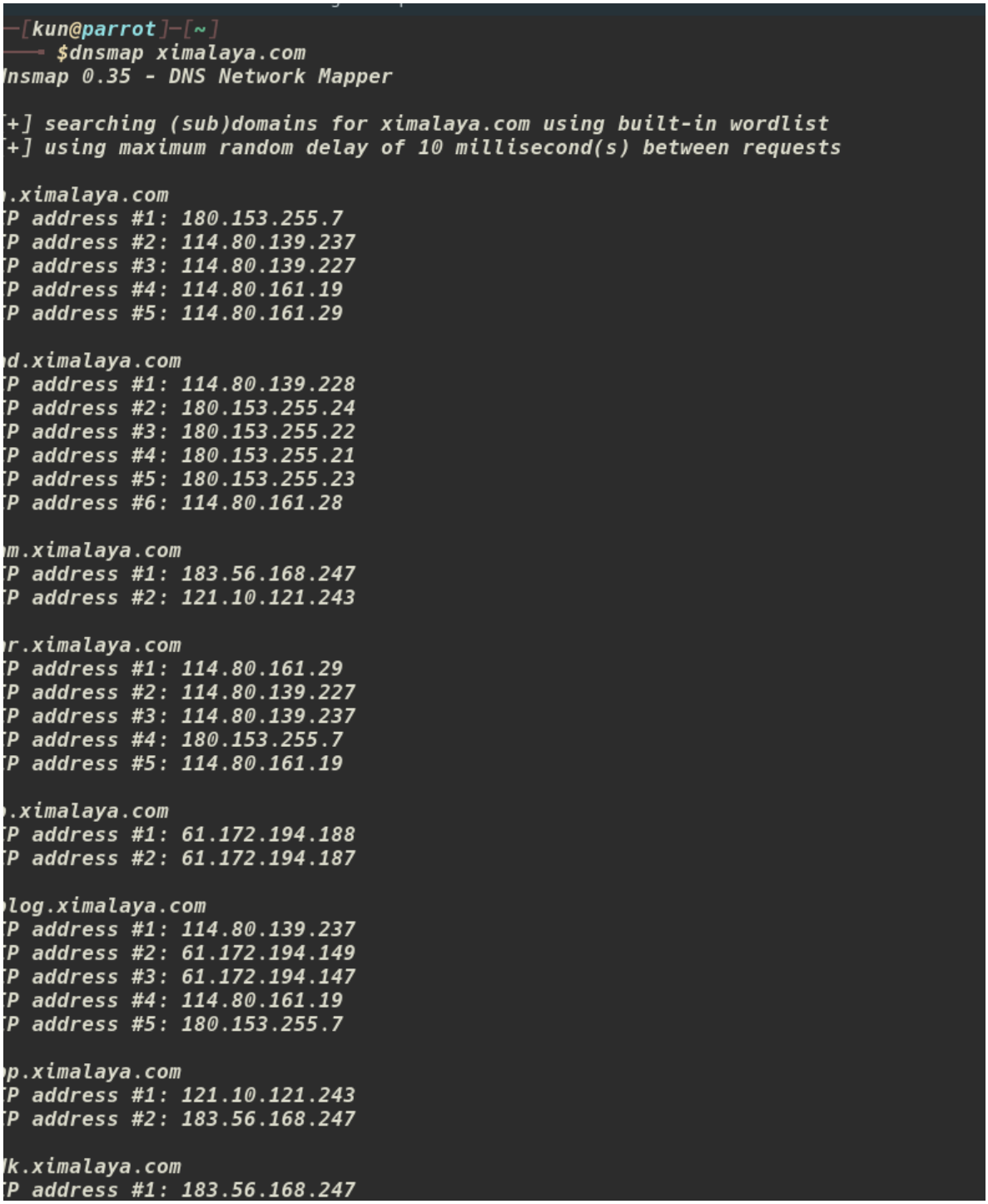
options:
-w
-r
-c
-d
-i (useful if you're obtaining false positives)

e.g.:
dnsmap example.com
dnsmap example.com -w yourwordlist.txt -r /tmp/domainbf_results.txt
dnsmap example.com -r /tmp/ -d 3000
dnsmap example.com -r ./domainbf_results.txt

二，命令范例

dnsmap ximalaya.com

枚举ximalaya.com相关的IP、网关、域名、子域等进行枚举。[^扫描需要时间，但是非常详细，根据目标的子域数目而决定，如果只有一个则一直等待。。]



> 以下是我扫描ximalaya.com的所有子域及DNS等信息。

```
dnsmap 0.35 - DNS Network Mapper

[+] searching (sub)domains for ximalaya.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

a.ximalaya.com
IP address #1: 180.153.255.7
IP address #2: 114.80.139.237
IP address #3: 114.80.139.227
IP address #4: 114.80.161.19
IP address #5: 114.80.161.29
```

```
ad.ximalaya.com
IP address #1: 114.80.139.228
IP address #2: 180.153.255.24
IP address #3: 180.153.255.22
IP address #4: 180.153.255.21
IP address #5: 180.153.255.23
IP address #6: 114.80.161.28

am.ximalaya.com
IP address #1: 183.56.168.247
IP address #2: 121.10.121.243

ar.ximalaya.com
IP address #1: 114.80.161.29
IP address #2: 114.80.139.227
IP address #3: 114.80.139.237
IP address #4: 180.153.255.7
IP address #5: 114.80.161.19

b.ximalaya.com
IP address #1: 61.172.194.188
IP address #2: 61.172.194.187

blog.ximalaya.com
IP address #1: 114.80.139.237
IP address #2: 61.172.194.149
IP address #3: 61.172.194.147
IP address #4: 114.80.161.19
IP address #5: 180.153.255.7

bp.ximalaya.com
IP address #1: 121.10.121.243
IP address #2: 183.56.168.247

dk.ximalaya.com
IP address #1: 183.56.168.247
IP address #2: 121.10.121.243

e.ximalaya.com
IP address #1: 114.80.139.237
IP address #2: 114.80.161.29
IP address #3: 114.80.161.19
IP address #4: 114.80.139.227
IP address #5: 180.153.255.7

fm.ximalaya.com
IP address #1: 114.80.139.237
IP address #2: 61.172.194.149
IP address #3: 114.80.161.19
IP address #4: 61.172.194.147
IP address #5: 180.153.255.7

help.ximalaya.com
IP address #1: 54.172.126.223
IP address #2: 34.206.241.1
IP address #3: 34.225.199.37
```

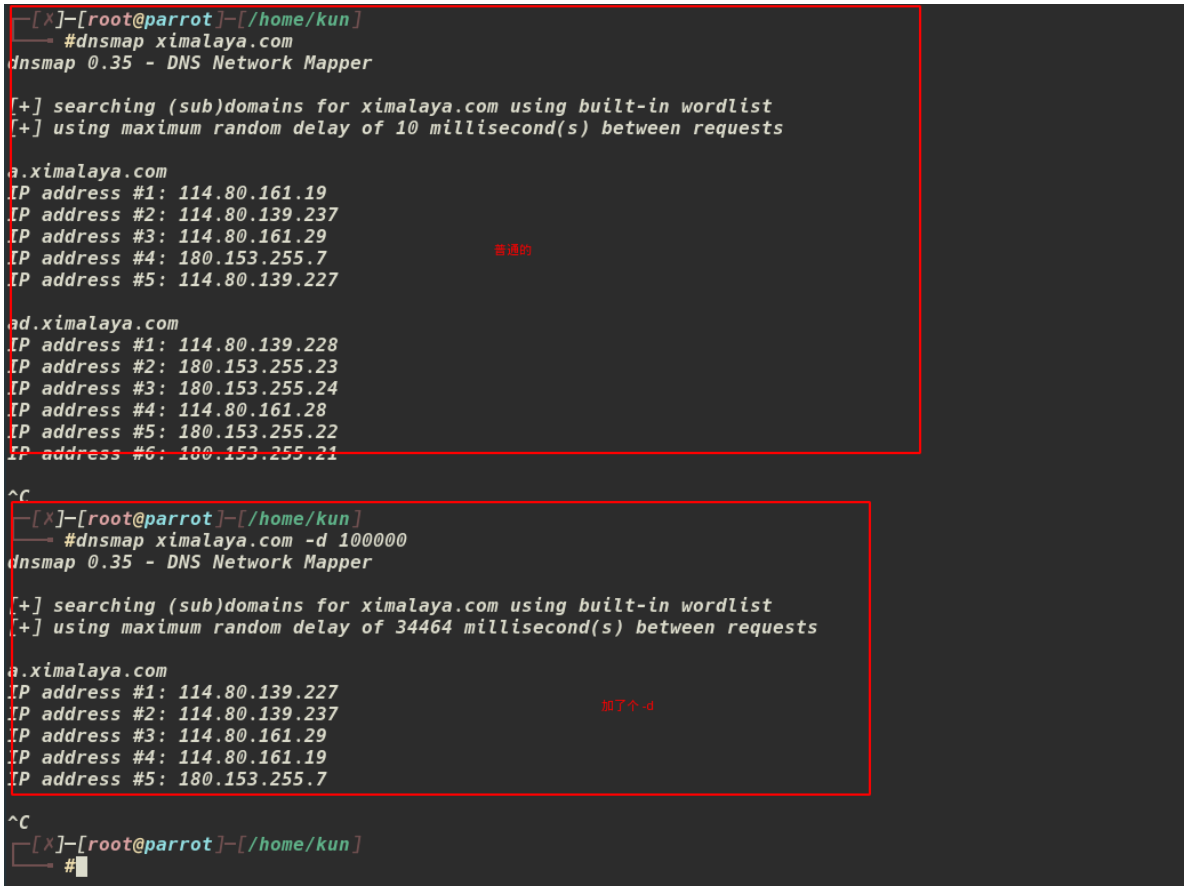
```
jt.ximalaya.com
IP address #1: 114.80.139.227
IP address #2: 114.80.139.237
IP address #3: 180.153.255.7
IP address #4: 114.80.161.29
IP address #5: 114.80.161.19

m.ximalaya.com
IP address #1: 114.80.139.227
IP address #2: 114.80.161.29
IP address #3: 114.80.161.19
IP address #4: 114.80.139.237
IP address #5: 180.153.255.7

ma.ximalaya.com
IP address #1: 180.153.255.7
IP address #2: 114.80.161.29
IP address #3: 114.80.139.237
IP address #4: 114.80.161.19
IP address #5: 114.80.139.227

mail.ximalaya.com
IP address #1: 114.80.143.2

mc.ximalaya.com
IP address #1: 114.80.161.19
IP address #2: 114.80.161.29
IP address #3: 114.80.139.237
IP address #4: 180.153.255.7
IP address #5: 114.80.139.227

mobile.ximalaya.com
IP address #1: 114.80.166.1
IP address #2: 114.80.142.163
IP address #3: 114.80.139.226
IP address #4: 114.80.166.7
IP address #5: 114.80.166.4
IP address #6: 114.80.139.230
IP address #7: 114.80.166.6
IP address #8: 114.80.161.18
IP address #9: 114.80.161.30

mp.ximalaya.com
IP address #1: 180.153.255.7
IP address #2: 114.80.161.19
IP address #3: 114.80.161.29
IP address #4: 114.80.139.227
IP address #5: 114.80.139.237

partners.ximalaya.com
IP address #1: 212.129.231.224

pc.ximalaya.com
IP address #1: 114.80.161.19
IP address #2: 114.80.139.237
IP address #3: 114.80.161.29
IP address #4: 180.153.255.7
IP address #5: 114.80.139.227
```

```
qf.ximalaya.com
IP address #1: 114.80.139.237
IP address #2: 61.172.194.147
IP address #3: 180.153.255.7
IP address #4: 114.80.161.19
IP address #5: 61.172.194.149

qm.ximalaya.com
IP address #1: 112.124.115.85

search.ximalaya.com
IP address #1: 114.80.161.19
IP address #2: 180.153.255.7
IP address #3: 114.80.139.237
IP address #4: 114.80.139.227
IP address #5: 114.80.161.29

test.ximalaya.com
IP address #1: 43.247.101.212

uat.ximalaya.com
IP address #1: 61.172.194.135

upload.ximalaya.com
IP address #1: 180.153.255.7
IP address #2: 114.80.139.237
IP address #3: 114.80.139.227
IP address #4: 114.80.161.29
IP address #5: 114.80.161.19

vpn.ximalaya.com
IP address #1: 43.247.101.218

www.ximalaya.com
IP address #1: 180.153.255.7
IP address #2: 114.80.161.19
IP address #3: 114.80.139.227
IP address #4: 114.80.139.237
IP address #5: 114.80.161.29

[+] 28 (sub)domains and 107 IP address(es) found
[+] completion time: 4750 second(s)
```

dnsmap ximalaya.com -d 100000

设置延迟毫秒为10000[^当然这个数值你可以自己定义的，我定义的是100000，你也可以定义为1也行]

> 这样做的好处就是你的Ip不会连续的发送多个握手包，会让服务器认为你是正常访问


┌──[x]─[root@parrot]─[/home/kun]
└──╼ #dnsmap ximalaya.com
dnsmap 0.35 - DNS Network Mapper
[+] searching (sub)domains for ximalaya.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests
a.ximalaya.com
IP address #1: 114.80.161.19
IP address #2: 114.80.139.237
IP address #3: 114.80.161.29
IP address #4: 180.153.255.7
IP address #5: 114.80.139.227
ad.ximalaya.com
IP address #1: 114.80.139.228
IP address #2: 180.153.255.23
IP address #3: 180.153.255.24
IP address #4: 114.80.161.28
IP address #5: 180.153.255.22
IP address #6: 180.153.255.21
普通的
^C
┌──[x]─[root@parrot]─[/home/kun]
└──╼ #dnsmap ximalaya.com -d 100000
dnsmap 0.35 - DNS Network Mapper
[+] searching (sub)domains for ximalaya.com using built-in wordlist
[+] using maximum random delay of 34464 millisecond(s) between requests
a.ximalaya.com
IP address #1: 114.80.139.227
IP address #2: 114.80.139.237
IP address #3: 114.80.161.29
IP address #4: 114.80.161.19
IP address #5: 180.153.255.7
加了个-d
^C
┌──[x]─[root@parrot]─[/home/kun]
└──╼ #