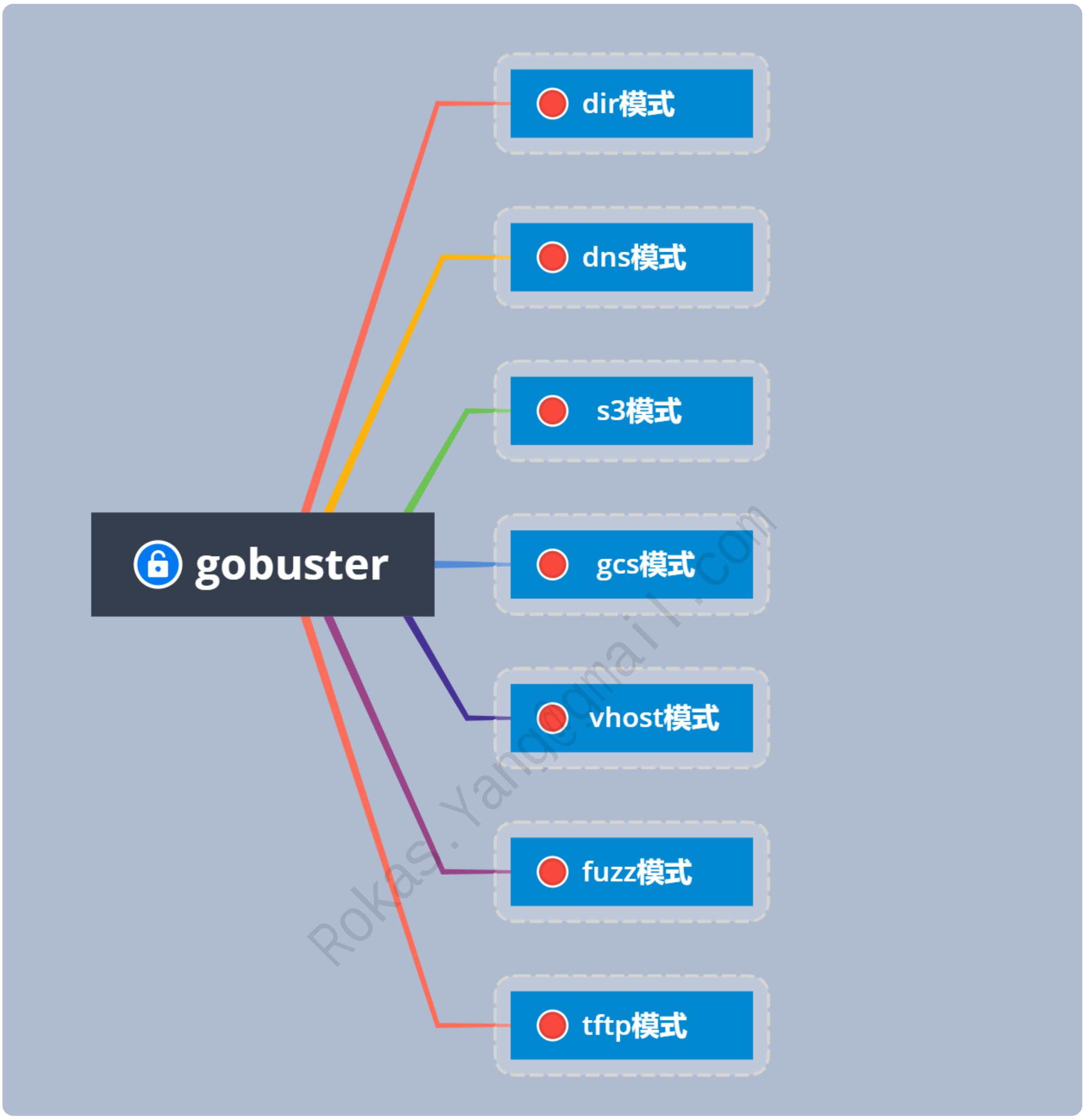
一、前言

Gobuster是一款用go语言编写的对于网站**目录/文件**、**DNS子域**、**虚拟主机vhost**进行暴力穷举的开源工具，常用于安全领域，其常用的暴力破解模式到目前为止（3.6版本）有如下几种：



模式	含义
dir	最经典的文件路径/目录破解模式。
dns	dns子域名破解模式。
s3	枚举打开S3存储桶并查找存在和存储桶清单（适用于aws）。
gcs	枚举打开的谷歌云存储桶。
vhost	虚拟主机枚举模式（不同于dns子域）。
fuzz	一些基本的模糊处理， 替代 FUZZ 关键字模式。
tftp	暴力破解tftp文件。

近期在某些场景中用到了gobuster，因此不妨趁热打铁写了本文作为沉淀。本文将从上面几种模式中选择最常见最具普遍性适用性的模式：**dir**、**dns**、**vhost**、**fuzz**模式中详细讲解其用法，**s3**和**gc3**适用于aws和谷歌云(gcp)的一些存储桶资源场景，详细用法可以通过 `gobuster help <mode>` 来查看。

二、全局参数

首先列举一下全局参数，这些参数在所有模式中都能被使用。

参数	含义
--debug	打开debug模式。
--delay duration	每个线程在请求之间等待的时间（举例： `--delay 1500ms` ）。
--no-color	禁用颜色输出。
--no-error	不显示错误。
-z|--no-progress	不显示进度。
-o|--output string	输出结果到文件。
-p|--pattern string	包含替换模式的文件。
-q|--quiet	安静模式，不打印banner信息和一些无用信息。
-t|--threads int	指定线程数量（默认10）。
-v|--verbose	详细输出日志（404状态码的也会展示）。
-w|--wordlist string	指定字典路径，指定 `-` 可以通过标准输入中读取。
--wordlist-offset int	从字典的指定位置继续（默认偏移量为0，从第一个开始）。

三、关于字典

字典是至关重要的一把钥匙，一个足够强大的字典能爆破出更多的可能性，如果要DIY字典则建议使用crunch生成，整理收集业内极具知名的字典如下：

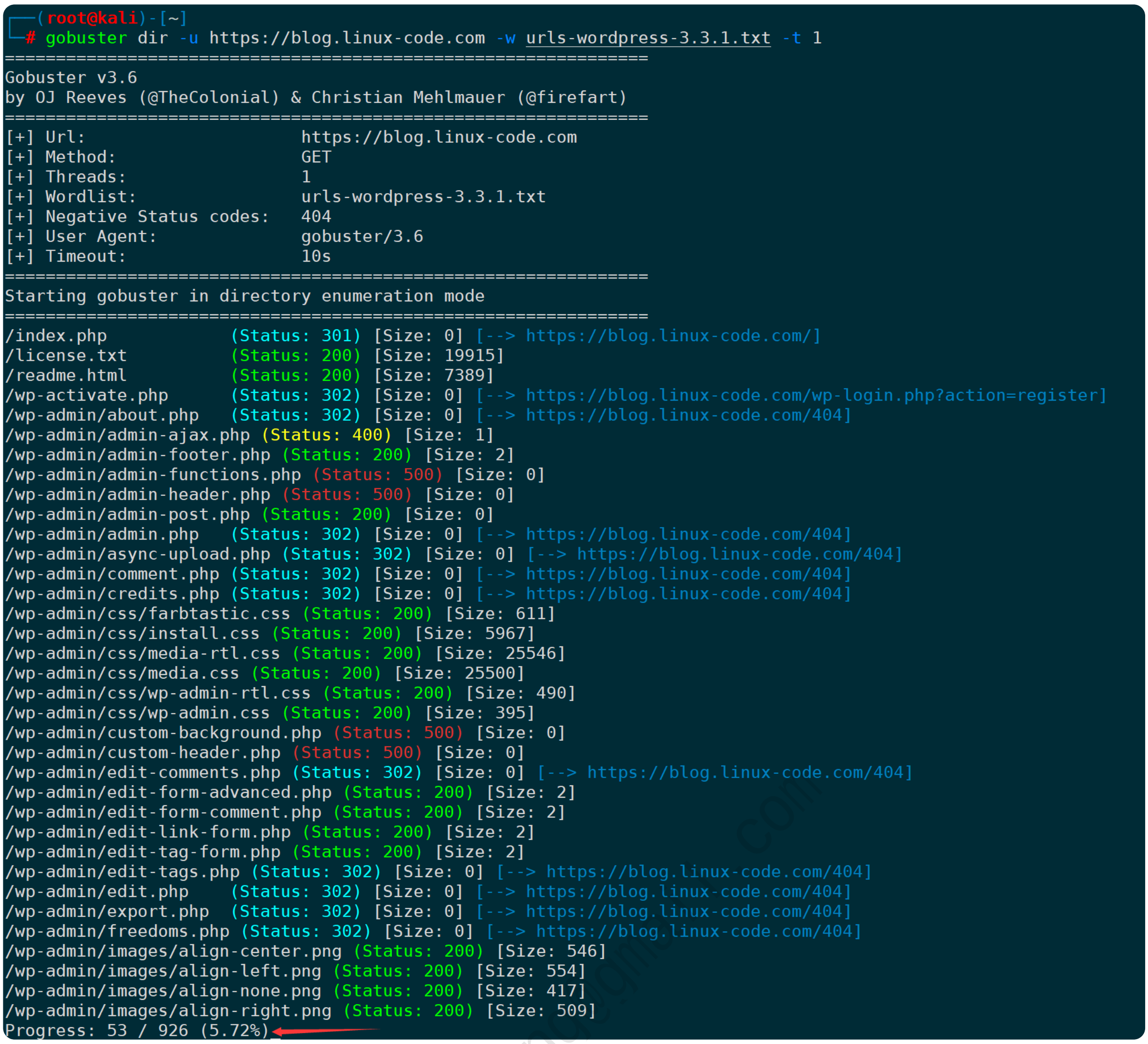
项目名称	链接
Fuzzing-Dicts	https://github.com/3had0w/Fuzzing-Dicts
weakpass	https://weakpass.com/
SecLists	https://github.com/danielmiessler/SecLists
Assetnote Wordlists	https://wordlists.assetnote.io/
fuzzdb	https://github.com/fuzzdb-project/fuzzdb
PayloadsAllTheThings	https://github.com/swisskyrepo/PayloadsAllTheThings
samlists	https://github.com/the-xentropy/samlists
Exploit-Dictionary	https://github.com/epony4c/Exploit-Dictionary

四、目录/文件路径暴力枚举（dir）

1.指定url链接枚举（-u|--url）

-u参数用来指定目标URL地址，此参数必选，同时配合全局参数里的-w来指定字典：

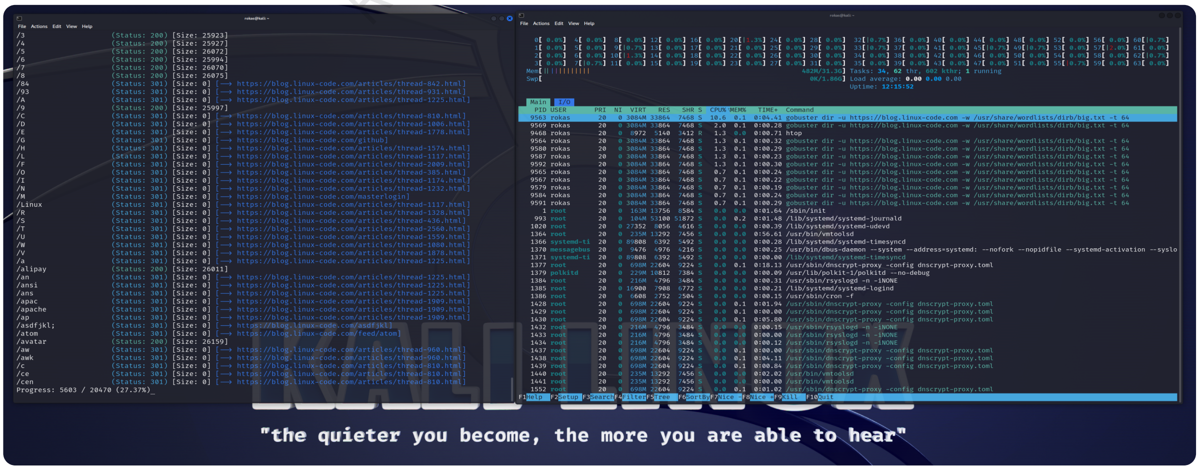
```
gobuster dir -u <URL> -w <wordlist>
```



```
┌──(root㉿kali)-[~]
└─# gobuster dir -u https://blog.linux-code.com -w urls-wordpress-3.3.1.txt -t 1
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://blog.linux-code.com
[+] Method:                  GET
[+] Threads:                 1
[+] Wordlist:                urls-wordpress-3.3.1.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 301) [Size: 0] [--> https://blog.linux-code.com/]
/license.txt          (Status: 200) [Size: 19915]
/readme.html          (Status: 200) [Size: 7389]
/wp-activate.php      (Status: 302) [Size: 0] [--> https://blog.linux-code.com/wp-login.php?action=register]
/wp-admin/about.php   (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/admin-ajax.php (Status: 400) [Size: 1]
/wp-admin/admin-footer.php (Status: 200) [Size: 2]
/wp-admin/admin-functions.php (Status: 500) [Size: 0]
/wp-admin/admin-header.php (Status: 500) [Size: 0]
/wp-admin/admin-post.php (Status: 200) [Size: 0]
/wp-admin/admin.php   (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/async-upload.php (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/comment.php (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/credits.php (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/css/farbtastic.css (Status: 200) [Size: 611]
/wp-admin/css/install.css (Status: 200) [Size: 5967]
/wp-admin/css/media-rtl.css (Status: 200) [Size: 25546]
/wp-admin/css/media.css (Status: 200) [Size: 25500]
/wp-admin/css/wp-admin-rtl.css (Status: 200) [Size: 490]
/wp-admin/css/wp-admin.css (Status: 200) [Size: 395]
/wp-admin/custom-background.php (Status: 500) [Size: 0]
/wp-admin/custom-header.php (Status: 500) [Size: 0]
/wp-admin/edit-comments.php (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/edit-form-advanced.php (Status: 200) [Size: 2]
/wp-admin/edit-form-comment.php (Status: 200) [Size: 2]
/wp-admin/edit-link-form.php (Status: 200) [Size: 2]
/wp-admin/edit-tag-form.php (Status: 200) [Size: 2]
/wp-admin/edit-tags.php (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/edit.php    (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/export.php  (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/freedoms.php (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/images/align-center.png (Status: 200) [Size: 546]
/wp-admin/images/align-left.png (Status: 200) [Size: 554]
/wp-admin/images/align-none.png (Status: 200) [Size: 417]
/wp-admin/images/align-right.png (Status: 200) [Size: 509]
Progress: 53 / 926 (5.72%)
```

默认使用10个线程，上图通过**-t 1**只指定了一个线程。

指定64个线程的效果如下：



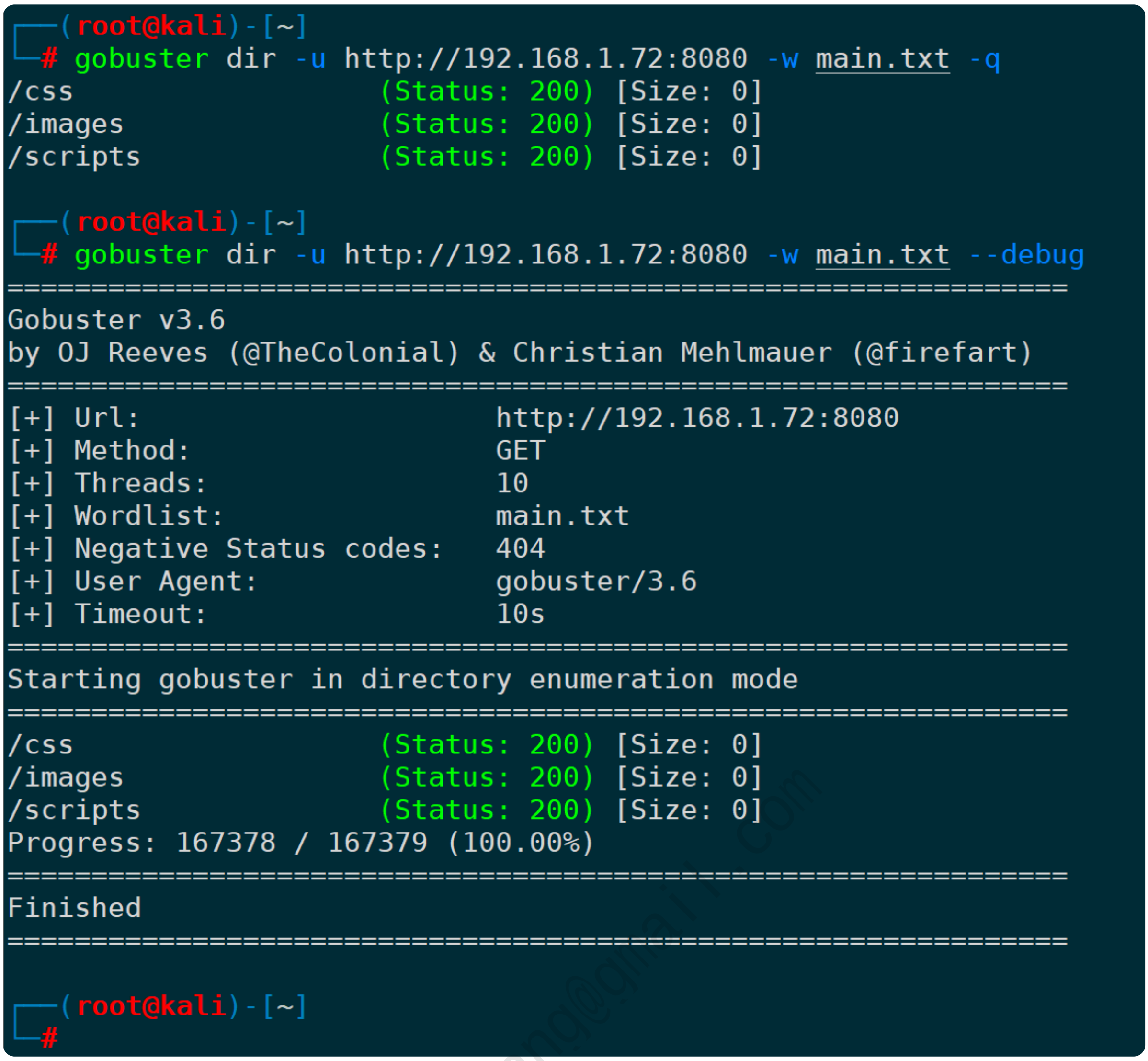
rokas@kali: ~
File Actions Edit View Help
rokas@kali: ~
File Actions Edit View Help
"the quieter you become, the more you are able to hear"

```
/3                    (Status: 200) [Size: 25923]
/4                    (Status: 200) [Size: 25927]
/5                    (Status: 200) [Size: 26072]
/6                    (Status: 200) [Size: 25994]
/7                    (Status: 200) [Size: 26070]
/8                    (Status: 200) [Size: 26075]
/84                   (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-842.html]
/93                   (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-931.html]
/A                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1225.html]
/9                    (Status: 200) [Size: 25997]
/C                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-810.html]
/D                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1006.html]
/E                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1778.html]
/G                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/github]
/H                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1574.html]
/L                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1117.html]
/F                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-2009.html]
/O                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-385.html]
/I                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1174.html]
/N                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1232.html]
/M                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/masterlogin]
/Linux                (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1117.html]
/R                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1328.html]
/S                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-436.html]
/T                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-2560.html]
/U                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1559.html]
/W                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1080.html]
/V                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1878.html]
/a                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1225.html]
/alipay               (Status: 200) [Size: 26011]
/an                   (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1225.html]
/ansi                 (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1225.html]
/ans                  (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1225.html]
/apac                 (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1909.html]
/apache               (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1909.html]
/ap                   (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-1909.html]
/asdfjkl;             (Status: 301) [Size: 0] [→ https://blog.linux-code.com/asdfjkl]
/atom                 (Status: 301) [Size: 0] [→ https://blog.linux-code.com/feed/atom]
/avatar               (Status: 200) [Size: 26159]
/aw                   (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-960.html]
/awk                  (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-960.html]
/c                    (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-810.html]
/ce                   (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-810.html]
/cen                  (Status: 301) [Size: 0] [→ https://blog.linux-code.com/articles/thread-810.html]
Progress: 5603 / 20470 (27.37%)_
```

```
    0[ 0.0%]  4[ 0.0%]  8[ 0.0%] 12[ 0.0%] 16[ 0.0%] 20[|1.3%] 24[ 0.0%] 28[ 0.0%]  32[|0.7%] 36[ 0.0%] 40[ 0.0%] 44[ 0.0%] 48[ 0.0%] 52[ 0.0%] 56[ 0.0%] 60[|0.7%]
    1[ 0.0%]  5[ 0.0%]  9[|0.7%] 13[ 0.0%] 17[ 0.0%] 21[ 0.0%] 25[ 0.0%] 29[ 0.0%]  33[|0.7%] 37[ 0.0%] 41[ 0.0%] 45[|0.7%] 49[|0.7%] 53[ 0.0%] 57[|2.0%] 61[ 0.0%]
    2[ 0.0%]  6[ 0.0%] 10[|1.3%] 14[ 0.0%] 18[ 0.0%] 22[ 0.0%] 26[ 0.0%] 30[ 0.0%]  34[ 0.0%] 38[ 0.0%] 42[ 0.0%] 46[ 0.0%] 50[ 0.0%] 54[ 0.0%] 58[ 0.0%] 62[|0.7%]
    3[ 0.0%]  7[|0.7%] 11[ 0.0%] 15[ 0.0%] 19[ 0.0%] 23[ 0.0%] 27[ 0.0%] 31[ 0.0%]  35[ 0.0%] 39[ 0.0%] 43[ 0.0%] 47[ 0.0%] 51[ 0.0%] 55[|0.7%] 59[ 0.0%] 63[ 0.0%]
  Mem[|| |||||||||||                         482M/31.3G] Tasks: 34, 62 thr, 602 kthr; 1 running
  Swp[                                         0K/1.86G] Load average: 0.00 0.00 0.00
                                                         Uptime: 12:15:52

  Main  I/O
    PID USER       PRI  NI  VIRT   RES   SHR S  CPU% MEM%   TIME+  Command
   9563 rokas       20   0 3084M 33864  7468 S  10.6  0.1  0:04.41 gobuster dir -u https://blog.linux-code.com -w /usr/share/wordlists/dirb/big.txt -t 64
   9569 rokas       20   0 3084M 33864  7468 S   2.0  0.1  0:00.28 gobuster dir -u https://blog.linux-code.com -w /usr/share/wordlists/dirb/big.txt -t 64
   9468 rokas       20   0  8972  5140  3412 R   1.3  0.0  0:00.71 htop
   9564 rokas       20   0 3084M 33864  7468 S   1.3  0.1  0:00.32 gobuster dir -u https://blog.linux-code.com -w /usr/share/wordlists/dirb/big.txt -t 64
   9580 rokas       20   0 3084M 33864  7468 S   1.3  0.1  0:00.29 gobuster dir -u https://blog.linux-code.com -w /usr/share/wordlists/dirb/big.txt -t 64
   9587 rokas       20   0 3084M 33864  7468 S   1.3  0.1  0:00.23 gobuster dir -u https://blog.linux-code.com -w /usr/share/wordlists/dirb/big.txt -t 64
   9592 rokas       20   0 3084M 33864  7468 S   1.3  0.1  0:00.30 gobuster dir -u https://blog.linux-code.com -w /usr/share/wordlists/dirb/big.txt -t 64
   9565 rokas       20   0 3084M 33864  7468 S   0.7  0.1  0:00.24 gobuster dir -u https://blog.linux-code.com -w /usr/share/wordlists/dirb/big.txt -t 64
   9567 rokas       20   0 3084M 33864  7468 S   0.7  0.1  0:00.22 gobuster dir -u https://blog.linux-code.com -w /usr/share/wordlists/dirb/big.txt -t 64
   9579 rokas       20   0 3084M 33864  7468 S   0.7  0.1  0:00.19 gobuster dir -u https://blog.linux-code.com -w /usr/share/wordlists/dirb/big.txt -t 64
   9584 rokas       20   0 3084M 33864  7468 S   0.7  0.1  0:00.24 gobuster dir -u https://blog.linux-code.com -w /usr/share/wordlists/dirb/big.txt -t 64
   9591 rokas       20   0 3084M 33864  7468 S   0.7  0.1  0:00.29 gobuster dir -u https://blog.linux-code.com -w /usr/share/wordlists/dirb/big.txt -t 64
      1 root        20   0  163M 13756  8584 S   0.0  0.0  0:01.64 /sbin/init
    993 root        20   0  104M 53100 51872 S   0.0  0.2  0:01.48 /lib/systemd/systemd-journald
   1020 root        20   0 27352  8056  4616 S   0.0  0.0  0:00.39 /lib/systemd/systemd-udevd
   1364 root        20   0  235M 13292  7456 S   0.0  0.0  0:56.61 /usr/bin/vmtoolsd
   1366 systemd-ti  20   0 89808  6392  5492 S   0.0  0.0  0:00.28 /lib/systemd/systemd-timesyncd
   1370 messagebus  20   0  9476  4976  4216 S   0.0  0.0  0:00.25 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslo
   1371 systemd-ti  20   0 89808  6392  5492 S   0.0  0.0  0:00.00 /lib/systemd/systemd-timesyncd
   1377 root        20   0  698M 22604  9224 S   0.0  0.1  0:18.13 /usr/sbin/dnscrypt-proxy -config dnscrypt-proxy.toml
   1379 polkitd     20   0  229M 10812  7384 S   0.0  0.0  0:00.09 /usr/lib/polkit-1/polkitd --no-debug
   1384 root        20   0  216M  4796  3484 S   0.0  0.0  0:00.31 /usr/sbin/rsyslogd -n -iNONE
   1385 root        20   0 16900  7908  6772 S   0.0  0.0  0:00.21 /lib/systemd/systemd-logind
   1386 root        20   0  6608  2752  2504 S   0.0  0.0  0:00.15 /usr/sbin/cron -f
   1428 root        20   0  698M 22604  9224 S   0.0  0.1  0:01.94 /usr/sbin/dnscrypt-proxy -config dnscrypt-proxy.toml
   1429 root        20   0  698M 22604  9224 S   0.0  0.1  0:00.00 /usr/sbin/dnscrypt-proxy -config dnscrypt-proxy.toml
   1430 root        20   0  698M 22604  9224 S   0.0  0.1  0:05.80 /usr/sbin/dnscrypt-proxy -config dnscrypt-proxy.toml
   1432 root        20   0  216M  4796  3484 S   0.0  0.0  0:00.15 /usr/sbin/rsyslogd -n -iNONE
   1433 root        20   0  216M  4796  3484 S   0.0  0.0  0:00.00 /usr/sbin/rsyslogd -n -iNONE
   1434 root        20   0  216M  4796  3484 S   0.0  0.0  0:00.12 /usr/sbin/rsyslogd -n -iNONE
   1437 root        20   0  698M 22604  9224 S   0.0  0.1  0:00.00 /usr/sbin/dnscrypt-proxy -config dnscrypt-proxy.toml
   1438 root        20   0  698M 22604  9224 S   0.0  0.1  0:04.11 /usr/sbin/dnscrypt-proxy -config dnscrypt-proxy.toml
   1439 root        20   0  698M 22604  9224 S   0.0  0.1  0:00.84 /usr/sbin/dnscrypt-proxy -config dnscrypt-proxy.toml
   1440 root        20   0  235M 13292  7456 S   0.0  0.0  0:02.02 /usr/bin/vmtoolsd
   1441 root        20   0  235M 13292  7456 S   0.0  0.0  0:00.00 /usr/bin/vmtoolsd
   1552 root        20   0  698M 22604  9224 S   0.0  0.1  0:01.02 /usr/sbin/dnscrypt-proxy -config dnscrypt-proxy.toml
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

同时对比下全局参数里的**--quiet**和**--debug**：

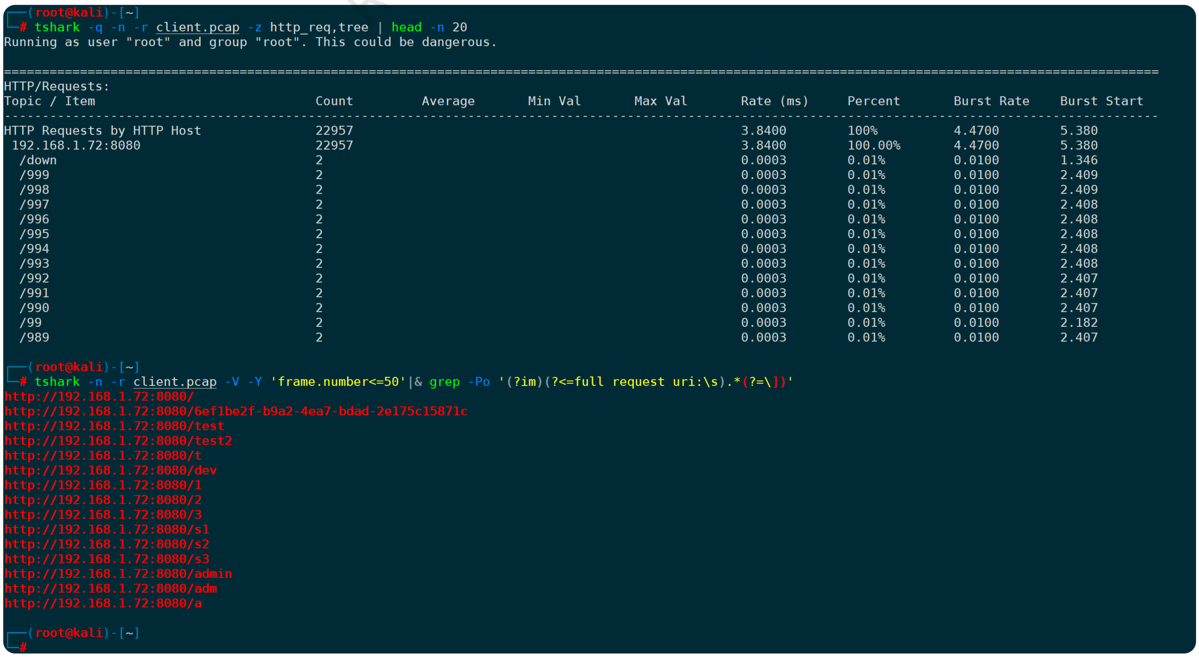
```
gobuster dir -u <URL> -w <wordlist> -q
gobuster dir -u <URL> -w <wordlist> --debug
```



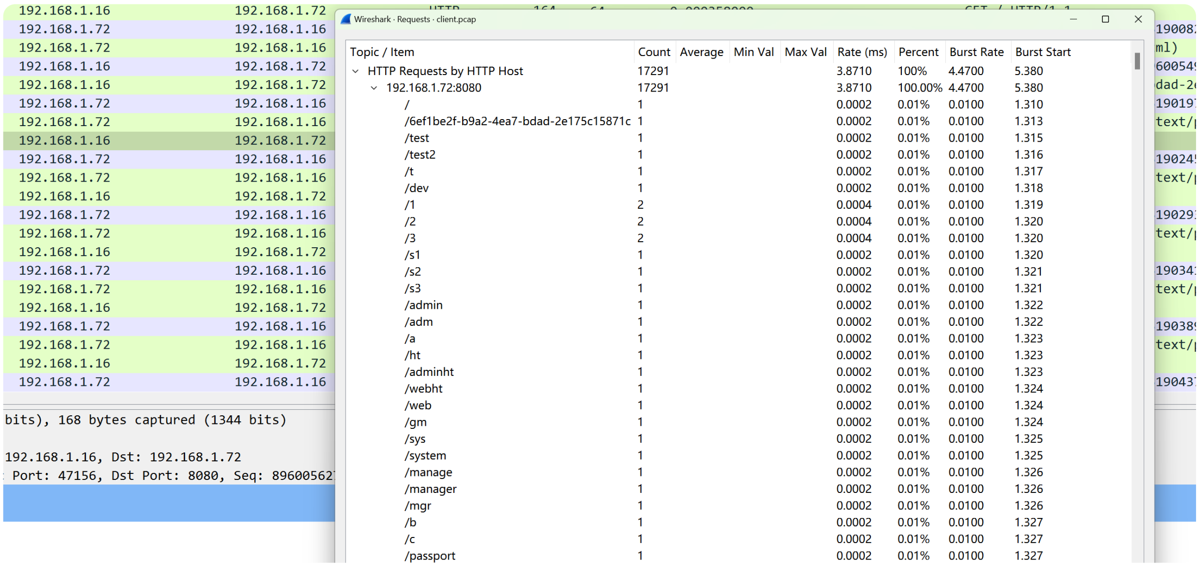
```
┌──(root@kali)-[~]
└─# gobuster dir -u http://192.168.1.72:8080 -w main.txt -q
/css                  (Status: 200) [Size: 0]
/images               (Status: 200) [Size: 0]
/scripts              (Status: 200) [Size: 0]

┌──(root@kali)-[~]
└─# gobuster dir -u http://192.168.1.72:8080 -w main.txt --debug
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.72:8080
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                main.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/css                  (Status: 200) [Size: 0]
/images               (Status: 200) [Size: 0]
/scripts              (Status: 200) [Size: 0]
Progress: 167378 / 167379 (100.00%)
===============================================================
Finished
===============================================================

┌──(root@kali)-[~]
└─#
```

如上图，不指定-q的情况下默认仍然是debug模式输出，会显示目的URL、HTTP方法、线程数量、字典文件、否定状态码（默认404）、UA信息、超时时间等。

通过抓包可以看到，gobuster根据字典里面的路径内容，组合成完整URL进行枚举：



```
┌──(root@kali)-[~]
└─# tshark -q -n -r client.pcap -z http_req,tree | head -n 20
Running as user "root" and group "root". This could be dangerous.

========================================================================================================================================================
HTTP/Requests:
Topic / Item                             Count         Average       Min Val       Max Val       Rate (ms)     Percent       Burst Rate    Burst Start
--------------------------------------------------------------------------------------------------------------------------------------------------------
HTTP Requests by HTTP Host               22957                                                   3.8400        100%          4.4700        5.380
 192.168.1.72:8080                       22957                                                   3.8400        100.00%       4.4700        5.380
  /down                                  2                                                       0.0003        0.01%         0.0100        1.346
  /999                                   2                                                       0.0003        0.01%         0.0100        2.409
  /998                                   2                                                       0.0003        0.01%         0.0100        2.409
  /997                                   2                                                       0.0003        0.01%         0.0100        2.408
  /996                                   2                                                       0.0003        0.01%         0.0100        2.408
  /995                                   2                                                       0.0003        0.01%         0.0100        2.408
  /994                                   2                                                       0.0003        0.01%         0.0100        2.408
  /993                                   2                                                       0.0003        0.01%         0.0100        2.408
  /992                                   2                                                       0.0003        0.01%         0.0100        2.407
  /991                                   2                                                       0.0003        0.01%         0.0100        2.407
  /990                                   2                                                       0.0003        0.01%         0.0100        2.407
  /99                                    2                                                       0.0003        0.01%         0.0100        2.182
  /989                                   2                                                       0.0003        0.01%         0.0100        2.407

┌──(root@kali)-[~]
└─# tshark -n -r client.pcap -V -Y 'frame.number<=50'|& grep -Po '(?im)(?<=full request uri:\s).*(?=\])'
http://192.168.1.72:8080/
http://192.168.1.72:8080/6ef1be2f-b9a2-4ea7-bdad-2e175c15871c
http://192.168.1.72:8080/test
http://192.168.1.72:8080/test2
http://192.168.1.72:8080/t
http://192.168.1.72:8080/dev
http://192.168.1.72:8080/1
http://192.168.1.72:8080/2
http://192.168.1.72:8080/3
http://192.168.1.72:8080/s1
http://192.168.1.72:8080/s2
http://192.168.1.72:8080/s3
http://192.168.1.72:8080/admin
http://192.168.1.72:8080/adm
http://192.168.1.72:8080/a

┌──(root@kali)-[~]
└─#
```



```
192.168.1.16        192.168.1.72
192.168.1.72        192.168.1.16
192.168.1.72        192.168.1.16
192.168.1.16        192.168.1.72
192.168.1.16        192.168.1.72
192.168.1.72        192.168.1.16
192.168.1.72        192.168.1.16
192.168.1.16        192.168.1.72
192.168.1.72        192.168.1.16
192.168.1.72        192.168.1.16
192.168.1.16        192.168.1.72
192.168.1.72        192.168.1.16
192.168.1.72        192.168.1.16
192.168.1.16        192.168.1.72
192.168.1.72        192.168.1.16
192.168.1.72        192.168.1.16
192.168.1.16        192.168.1.72
192.168.1.72        192.168.1.16
192.168.1.72        192.168.1.16
192.168.1.16        192.168.1.72
192.168.1.72        192.168.1.16

bits), 168 bytes captured (1344 bits)

192.168.1.16, Dst: 192.168.1.72
 Port: 47156, Dst Port: 8080, Seq: 89600562
```

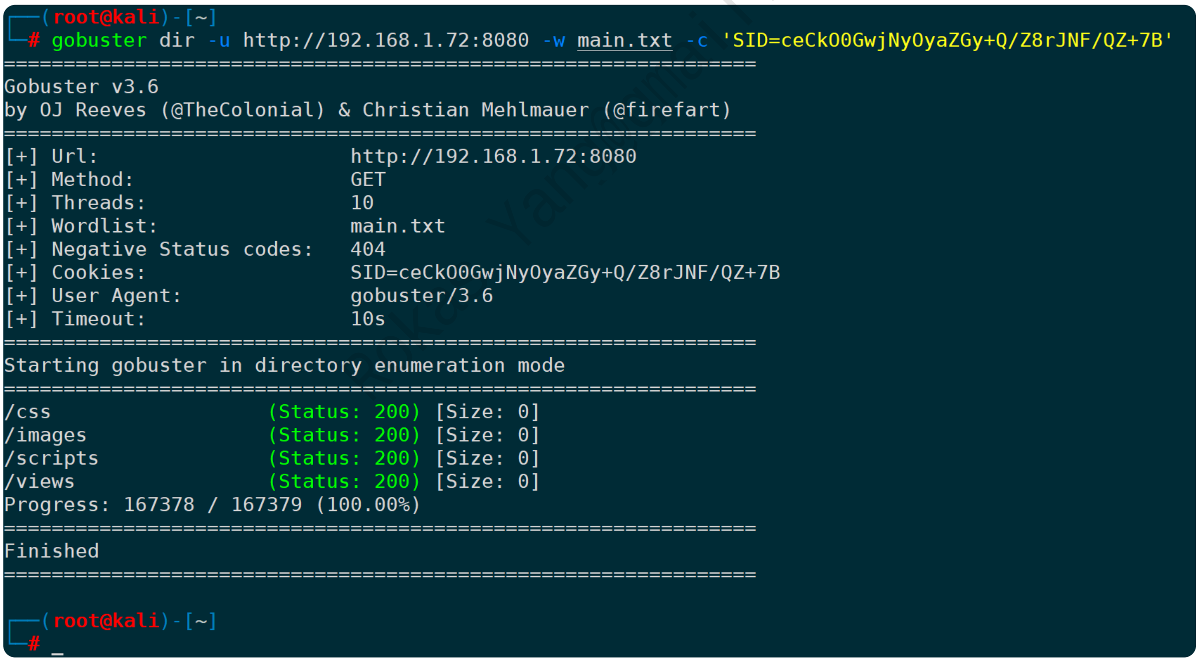
Wireshark · Requests · client.pcap

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
HTTP Requests by HTTP Host	17291				3.8710	100%	4.4700	5.380
192.168.1.72:8080	17291				3.8710	100.00%	4.4700	5.380
/	1				0.0002	0.01%	0.0100	1.310
/6ef1be2f-b9a2-4ea7-bdad-2e175c15871c	1				0.0002	0.01%	0.0100	1.313
/test	1				0.0002	0.01%	0.0100	1.315
/test2	1				0.0002	0.01%	0.0100	1.316
/t	1				0.0002	0.01%	0.0100	1.317
/dev	1				0.0002	0.01%	0.0100	1.318
/1	2				0.0004	0.01%	0.0100	1.319
/2	2				0.0004	0.01%	0.0100	1.320
/3	2				0.0004	0.01%	0.0100	1.320
/s1	1				0.0002	0.01%	0.0100	1.320
/s2	1				0.0002	0.01%	0.0100	1.321
/s3	1				0.0002	0.01%	0.0100	1.321
/admin	1				0.0002	0.01%	0.0100	1.322
/adm	1				0.0002	0.01%	0.0100	1.322
/a	1				0.0002	0.01%	0.0100	1.323
/ht	1				0.0002	0.01%	0.0100	1.323
/adminht	1				0.0002	0.01%	0.0100	1.323
/webht	1				0.0002	0.01%	0.0100	1.324
/web	1				0.0002	0.01%	0.0100	1.324
/gm	1				0.0002	0.01%	0.0100	1.324
/sys	1				0.0002	0.01%	0.0100	1.325
/system	1				0.0002	0.01%	0.0100	1.325
/manage	1				0.0002	0.01%	0.0100	1.326
/manager	1				0.0002	0.01%	0.0100	1.326
/mgr	1				0.0002	0.01%	0.0100	1.326
/b	1				0.0002	0.01%	0.0100	1.327
/c	1				0.0002	0.01%	0.0100	1.327
/passport	1				0.0002	0.01%	0.0100	1.327

因此确保字典足够强大，可能结果也会更多。

2.使用cookies（-c|--cookies）

```
gobuster dir -u <URL> -w <wordlist> -c <cookie>
```



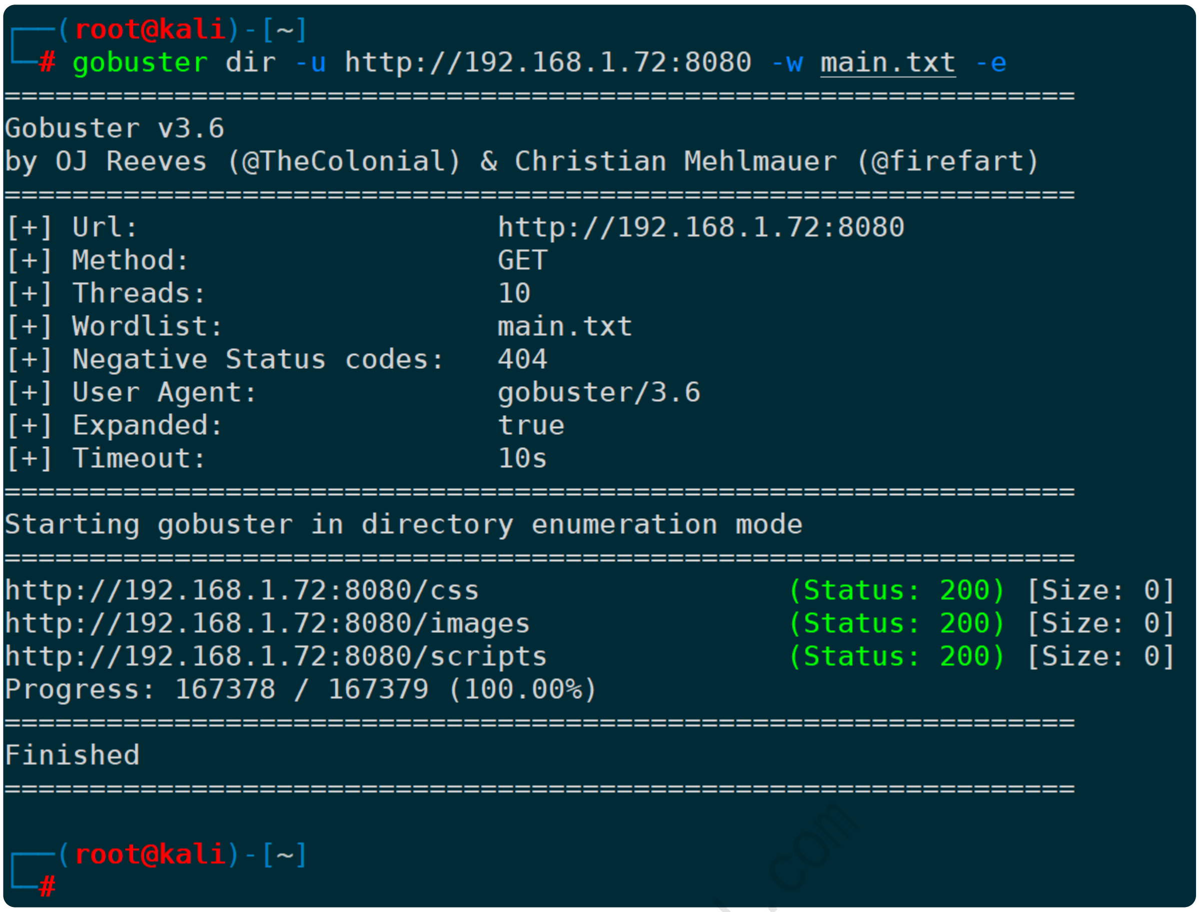
```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://192.168.1.72:8080 -w main.txt -c 'SID=ceCkO0GwjNyOyaZGy+Q/Z8rJNF/QZ+7B'
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.72:8080
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                main.txt
[+] Negative Status codes:   404
[+] Cookies:                 SID=ceCkO0GwjNyOyaZGy+Q/Z8rJNF/QZ+7B
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/css                  (Status: 200) [Size: 0]
/images               (Status: 200) [Size: 0]
/scripts              (Status: 200) [Size: 0]
/views                (Status: 200) [Size: 0]
Progress: 167378 / 167379 (100.00%)
===============================================================
Finished
===============================================================

┌──(root㉿kali)-[~]
└─# _
```

相当于拿到登录状态信息，再去枚举URL下的目录和文件。

3.打印完整URL（-e|--expanded）

默认只显示文件路径，通过-e参数可以将枚举出来的目录补全后以完整的URL显示：

```
gobuster dir -u <URL> -w <wordlist> -e
```

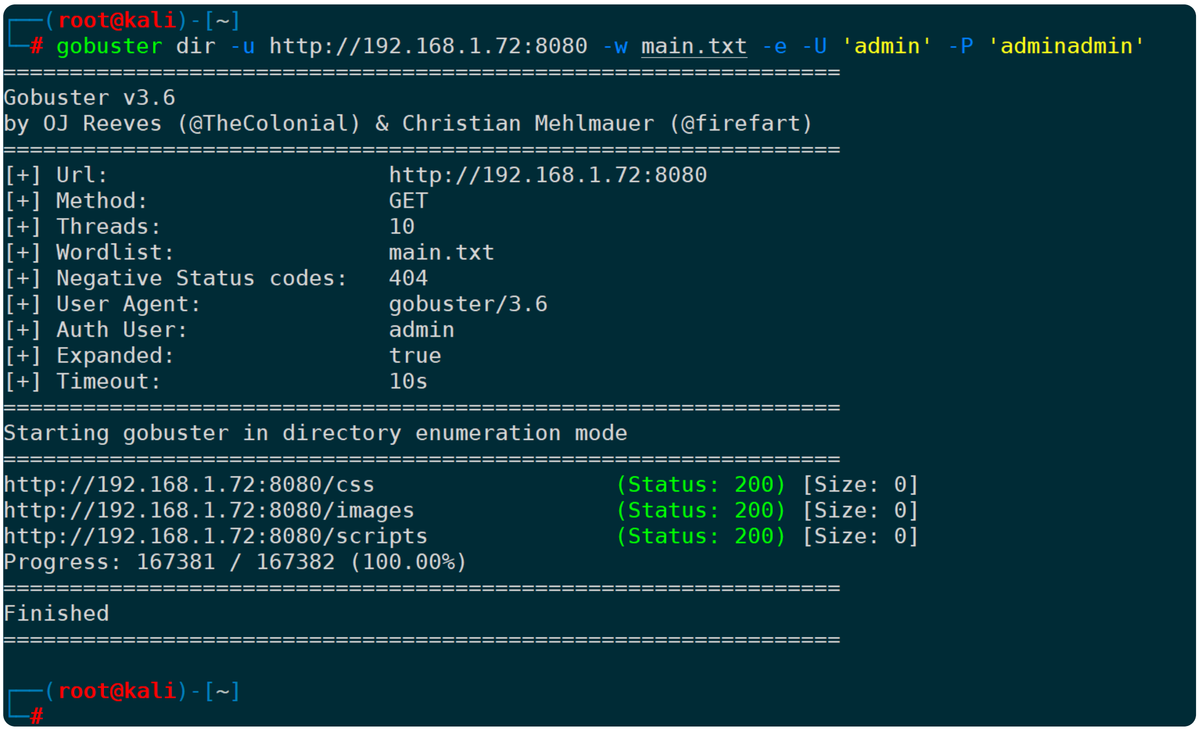


```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://192.168.1.72:8080 -w main.txt -e
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.72:8080
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                main.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
http://192.168.1.72:8080/css                 (Status: 200) [Size: 0]
http://192.168.1.72:8080/images              (Status: 200) [Size: 0]
http://192.168.1.72:8080/scripts             (Status: 200) [Size: 0]
Progress: 167378 / 167379 (100.00%)
===============================================================
Finished
===============================================================

┌──(root㉿kali)-[~]
└─#
```

4.指定用户名和密码（-U,--username|-P,--pasword）

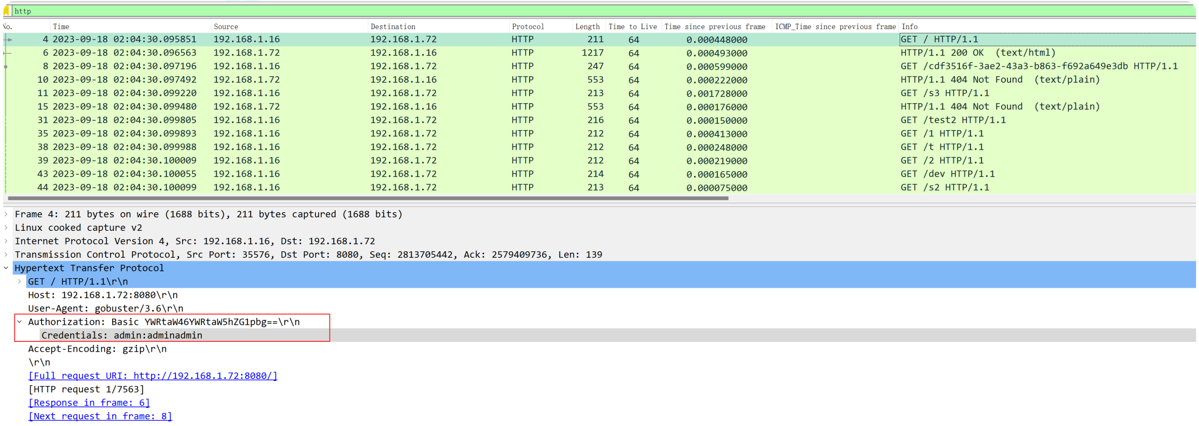
不想通过cookie的方式来获取，则可以携带用户名密码：

```
gobuster dir -u <URL> -w <wordlist> -e -U 'username' -P 'password'
```



```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://192.168.1.72:8080 -w main.txt -e -U 'admin' -P 'adminadmin'
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.72:8080
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                main.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Auth User:               admin
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
http://192.168.1.72:8080/css                 (Status: 200) [Size: 0]
http://192.168.1.72:8080/images              (Status: 200) [Size: 0]
http://192.168.1.72:8080/scripts             (Status: 200) [Size: 0]
Progress: 167381 / 167382 (100.00%)
===============================================================
Finished
===============================================================

┌──(root㉿kali)-[~]
└─#
```

通过抓包不难发现，这两个参数用的是基础鉴权，如果非基础鉴权则使用无效，会在HTTP头部里面携带基础鉴权的账号密码信息：



http

No.	Time	Source	Destination	Protocol	Length	Time to Live	Time since previous frame	ICMP_Time since previous frame	Info
4	2023-09-18 02:04:30.095851	192.168.1.16	192.168.1.72	HTTP	211	64	0.000448000		GET / HTTP/1.1
6	2023-09-18 02:04:30.096563	192.168.1.72	192.168.1.16	HTTP	1217	64	0.000493000		HTTP/1.1 200 OK (text/html)
8	2023-09-18 02:04:30.097196	192.168.1.16	192.168.1.72	HTTP	247	64	0.000599000		GET /cdf3516f-3ae2-43a3-b863-f692a649e3db HTTP/1.1
10	2023-09-18 02:04:30.097492	192.168.1.72	192.168.1.16	HTTP	553	64	0.000222000		HTTP/1.1 404 Not Found (text/plain)
11	2023-09-18 02:04:30.099220	192.168.1.16	192.168.1.72	HTTP	213	64	0.001728000		GET /s3 HTTP/1.1
15	2023-09-18 02:04:30.099480	192.168.1.72	192.168.1.16	HTTP	553	64	0.000176000		HTTP/1.1 404 Not Found (text/plain)
31	2023-09-18 02:04:30.099805	192.168.1.16	192.168.1.72	HTTP	216	64	0.000150000		GET /test2 HTTP/1.1
35	2023-09-18 02:04:30.099893	192.168.1.16	192.168.1.72	HTTP	212	64	0.000413000		GET /1 HTTP/1.1
38	2023-09-18 02:04:30.099988	192.168.1.16	192.168.1.72	HTTP	212	64	0.000248000		GET /t HTTP/1.1
39	2023-09-18 02:04:30.100009	192.168.1.16	192.168.1.72	HTTP	212	64	0.000219000		GET /2 HTTP/1.1
43	2023-09-18 02:04:30.100055	192.168.1.16	192.168.1.72	HTTP	214	64	0.000165000		GET /dev HTTP/1.1
44	2023-09-18 02:04:30.100099	192.168.1.16	192.168.1.72	HTTP	213	64	0.000075000		GET /s2 HTTP/1.1

```
> Frame 4: 211 bytes on wire (1688 bits), 211 bytes captured (1688 bits)
> Linux cooked capture v2
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.72
> Transmission Control Protocol, Src Port: 35576, Dst Port: 8080, Seq: 2813705442, Ack: 2579409736, Len: 139
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: 192.168.1.72:8080\r\n
    User-Agent: gobuster/3.6\r\n
  v Authorization: Basic YWRtaW46YWRtaW5hZG1pbg==\r\n
      Credentials: admin:adminadmin
    Accept-Encoding: gzip\r\n
    \r\n
    [Full request URI: http://192.168.1.72:8080/]
    [HTTP request 1/7563]
    [Response in frame: 6]
    [Next request in frame: 8]
```

5.忽略TLS/SSL证书验证（-k|--no-tls-validation）

curl、wget等七层工具也有一样的参数，忽略证书问题，不进行证书可用性校验：

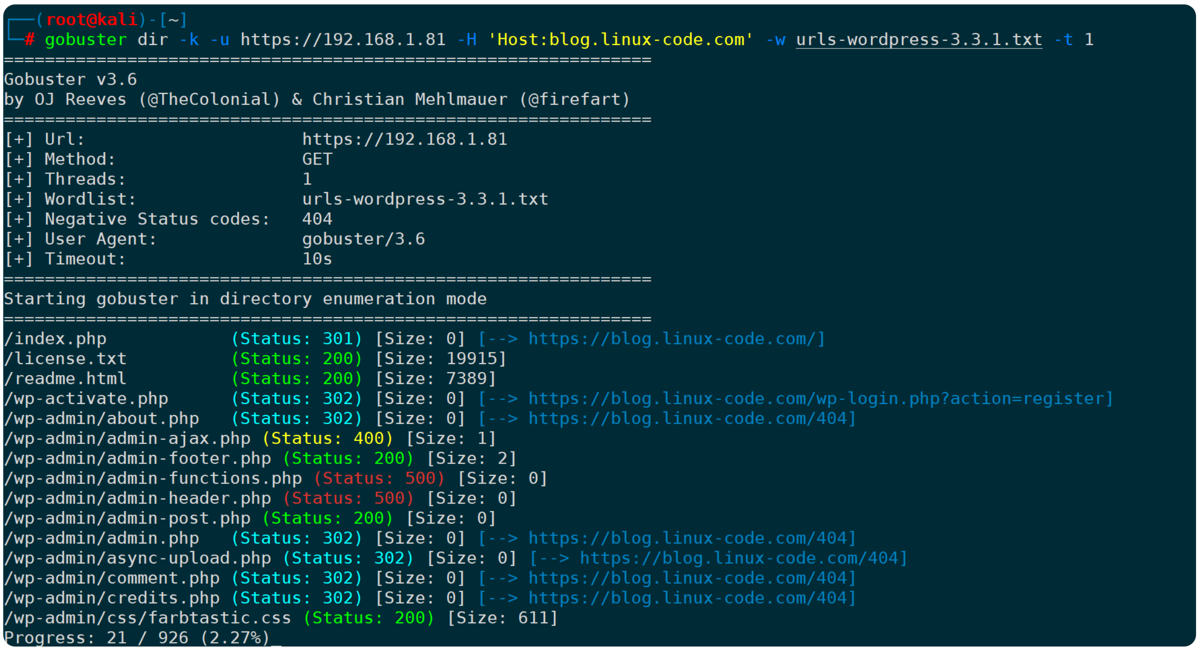
```
gobuster dir -k -u <URL> -H 'Host:<HOST>' -w <wordlist>
```

6.自定义http头部（-H|--headers）

通过-H参数指定http头部，可以模拟任何想要发送出去的HTTP头部字段。

比如指定特定HOST：

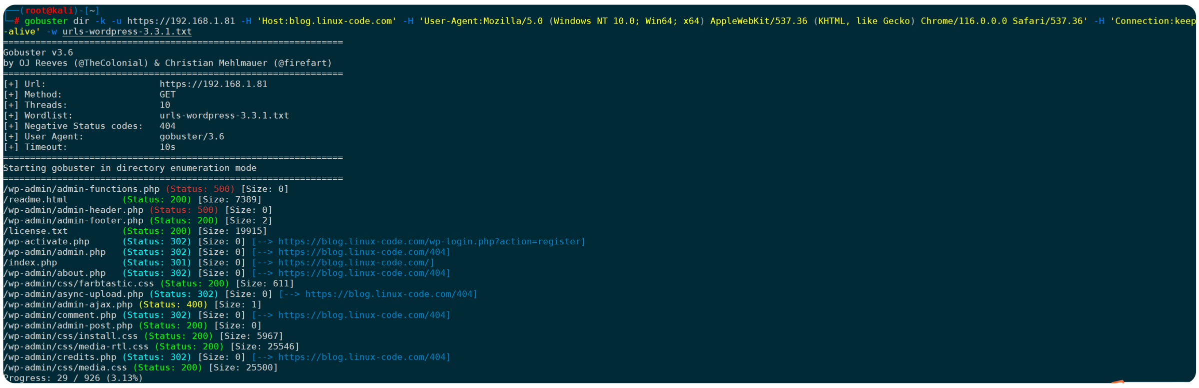
```
gobuster dir -k -u <URL> -H 'Host:<HOST>' -w <wordlist> -t 1
```



```
┌──(root㉿kali)-[~]
└─# gobuster dir -k -u https://192.168.1.81 -H 'Host:blog.linux-code.com' -w urls-wordpress-3.3.1.txt -t 1
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://192.168.1.81
[+] Method:                  GET
[+] Threads:                 1
[+] Wordlist:                urls-wordpress-3.3.1.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 301) [Size: 0] [--> https://blog.linux-code.com/]
/license.txt          (Status: 200) [Size: 19915]
/readme.html          (Status: 200) [Size: 7389]
/wp-activate.php      (Status: 302) [Size: 0] [--> https://blog.linux-code.com/wp-login.php?action=register]
/wp-admin/about.php   (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/admin-ajax.php (Status: 400) [Size: 1]
/wp-admin/admin-footer.php (Status: 200) [Size: 2]
/wp-admin/admin-functions.php (Status: 500) [Size: 0]
/wp-admin/admin-header.php (Status: 500) [Size: 0]
/wp-admin/admin-post.php (Status: 200) [Size: 0]
/wp-admin/admin.php   (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/async-upload.php (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/comment.php (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/credits.php (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/css/farbtastic.css (Status: 200) [Size: 611]
Progress: 21 / 926 (2.27%)_
```

指定多个头部，用多个-H分割，比如同时指定**Host**、**User-Agent**、**Connection**：

```
gobuster dir -k -u <URL> -H 'Host:<Host>' -H 'User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36' -H 'Connection:keep-alive' -w <wordlist>
```



```
┌──(root㉿kali)-[~]
└─# gobuster dir -k -u https://192.168.1.81 -H 'Host:blog.linux-code.com' -H 'User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36' -H 'Connection:keep
-alive' -w urls-wordpress-3.3.1.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://192.168.1.81
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                urls-wordpress-3.3.1.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/wp-admin/admin-functions.php (Status: 500) [Size: 0]
/readme.html          (Status: 200) [Size: 7389]
/wp-admin/admin-header.php (Status: 500) [Size: 0]
/wp-admin/admin-footer.php (Status: 200) [Size: 2]
/license.txt          (Status: 200) [Size: 19915]
/wp-activate.php      (Status: 302) [Size: 0] [--> https://blog.linux-code.com/wp-login.php?action=register]
/wp-admin/admin.php   (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/index.php            (Status: 301) [Size: 0] [--> https://blog.linux-code.com/]
/wp-admin/about.php   (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/css/farbtastic.css (Status: 200) [Size: 611]
/wp-admin/async-upload.php (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/admin-ajax.php (Status: 400) [Size: 1]
/wp-admin/comment.php (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/admin-post.php (Status: 200) [Size: 0]
/wp-admin/css/install.css (Status: 200) [Size: 5967]
/wp-admin/css/media-rtl.css (Status: 200) [Size: 25546]
/wp-admin/credits.php (Status: 302) [Size: 0] [--> https://blog.linux-code.com/404]
/wp-admin/css/media.css (Status: 200) [Size: 25500]
Progress: 29 / 926 (3.13%)
```

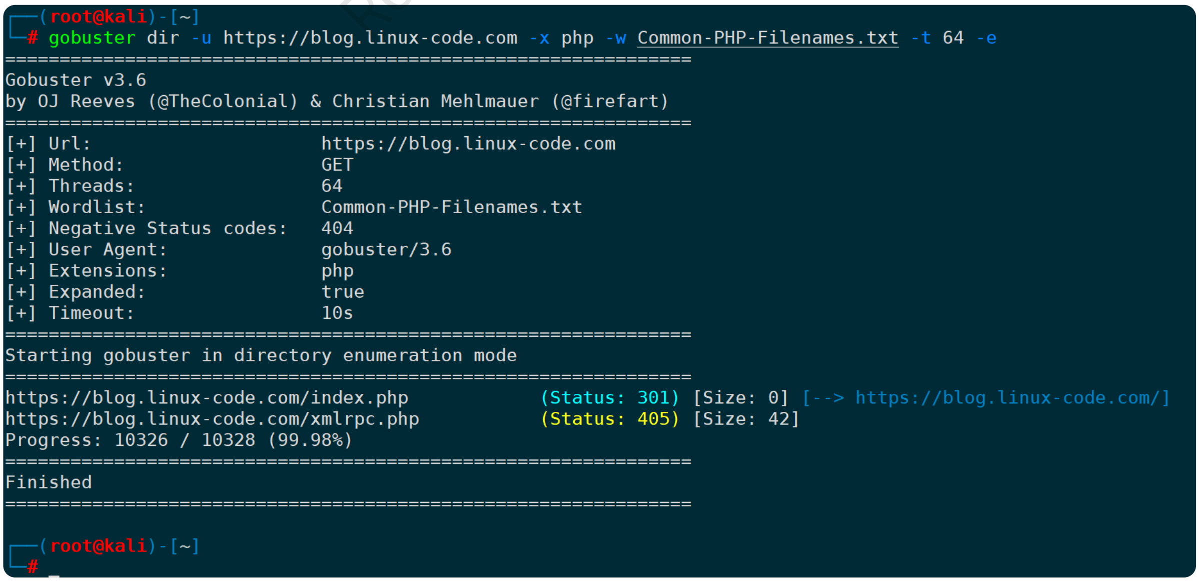
当然User-Agent也可以单独通过**-a|----useragent**来指定，gobuster提供了此参数，默认为：**gobuster/3.6**，后面的数字为版本号。

7.指定文件扩展名搜索（-x）

当只想搜索php时，使用**-x php**，搜索txt时，则指定**-x txt**，以此类推。

比如只搜索php的文件，显示完整URL（**-e**），指定64个线程（**-t 64**）：

```
gobuster dir -u <URL> -x php -w <wordlist> -t 64 -e
```

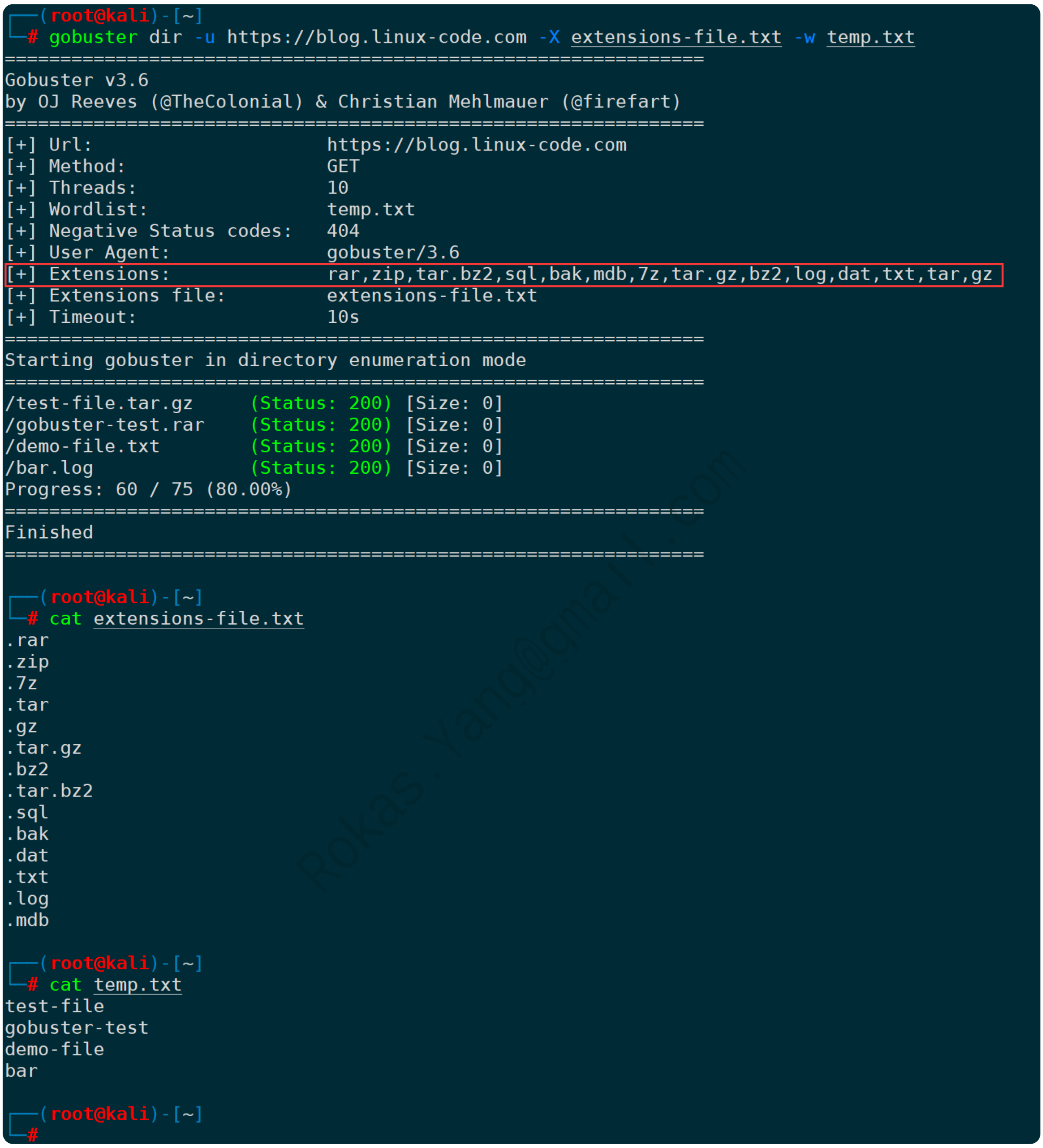


```
┌──(root㉿kali)-[~]
└─# gobuster dir -u https://blog.linux-code.com -x php -w Common-PHP-Filenames.txt -t 64 -e
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://blog.linux-code.com
[+] Method:                  GET
[+] Threads:                 64
[+] Wordlist:                Common-PHP-Filenames.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
https://blog.linux-code.com/index.php            (Status: 301) [Size: 0] [--> https://blog.linux-code.com/]
https://blog.linux-code.com/xmlrpc.php           (Status: 405) [Size: 42]
Progress: 10326 / 10328 (99.98%)
===============================================================
Finished
===============================================================

┌──(root㉿kali)-[~]
└─# _
```

8.读取要从文件搜索的扩展名（-X）

当要搜索的扩展名有多个时，可以通过读取扩展名的文件，不需要一个个手动指定：

```
gobuster dir -u <URL> -X <extensions-file> -w <wordlist>
```

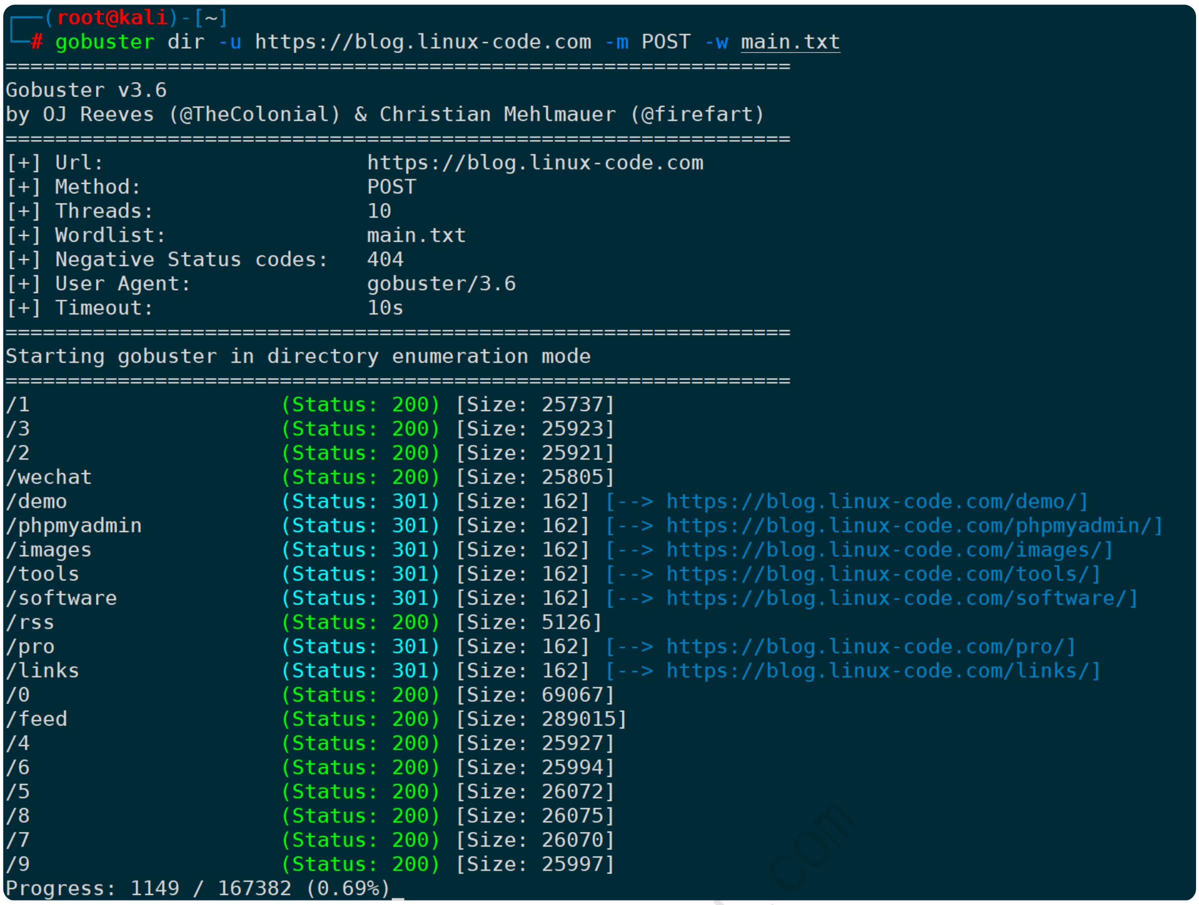


```
┌──(root@kali)-[~]
└─# gobuster dir -u https://blog.linux-code.com -X extensions-file.txt -w temp.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://blog.linux-code.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                temp.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              rar,zip,tar.bz2,sql,bak,mdb,7z,tar.gz,bz2,log,dat,txt,tar,gz
[+] Extensions file:         extensions-file.txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/test-file.tar.gz      (Status: 200) [Size: 0]
/gobuster-test.rar     (Status: 200) [Size: 0]
/demo-file.txt         (Status: 200) [Size: 0]
/bar.log               (Status: 200) [Size: 0]
Progress: 60 / 75 (80.00%)
===============================================================
Finished
===============================================================

┌──(root@kali)-[~]
└─# cat extensions-file.txt
.rar
.zip
.7z
.tar
.gz
.tar.gz
.bz2
.tar.bz2
.sql
.bak
.dat
.txt
.log
.mdb

┌──(root@kali)-[~]
└─# cat temp.txt
test-file
gobuster-test
demo-file
bar

┌──(root@kali)-[~]
└─#
```

9.指定HTTP请求方法（-m|--method）

不指定默认为GET，如果需要指定其它HTTP方法，则通过-m指定，譬如指定POST请求可以是：

```
gobuster dir -u <URL> -m POST -w <wordlist>
```



```
┌──(root@kali)-[~]
└─# gobuster dir -u https://blog.linux-code.com -m POST -w main.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://blog.linux-code.com
[+] Method:                  POST
[+] Threads:                 10
[+] Wordlist:                main.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/1                    (Status: 200) [Size: 25737]
/3                    (Status: 200) [Size: 25923]
/2                    (Status: 200) [Size: 25921]
/wechat               (Status: 200) [Size: 25805]
/demo                 (Status: 301) [Size: 162] [--> https://blog.linux-code.com/demo/]
/phpmyadmin           (Status: 301) [Size: 162] [--> https://blog.linux-code.com/phpmyadmin/]
/images               (Status: 301) [Size: 162] [--> https://blog.linux-code.com/images/]
/tools                (Status: 301) [Size: 162] [--> https://blog.linux-code.com/tools/]
/software             (Status: 301) [Size: 162] [--> https://blog.linux-code.com/software/]
/rss                  (Status: 200) [Size: 5126]
/pro                  (Status: 301) [Size: 162] [--> https://blog.linux-code.com/pro/]
/links                (Status: 301) [Size: 162] [--> https://blog.linux-code.com/links/]
/0                    (Status: 200) [Size: 69067]
/feed                 (Status: 200) [Size: 289015]
/4                    (Status: 200) [Size: 25927]
/6                    (Status: 200) [Size: 25994]
/5                    (Status: 200) [Size: 26072]
/8                    (Status: 200) [Size: 26075]
/7                    (Status: 200) [Size: 26070]
/9                    (Status: 200) [Size: 25997]
Progress: 1149 / 167382 (0.69%)_
```

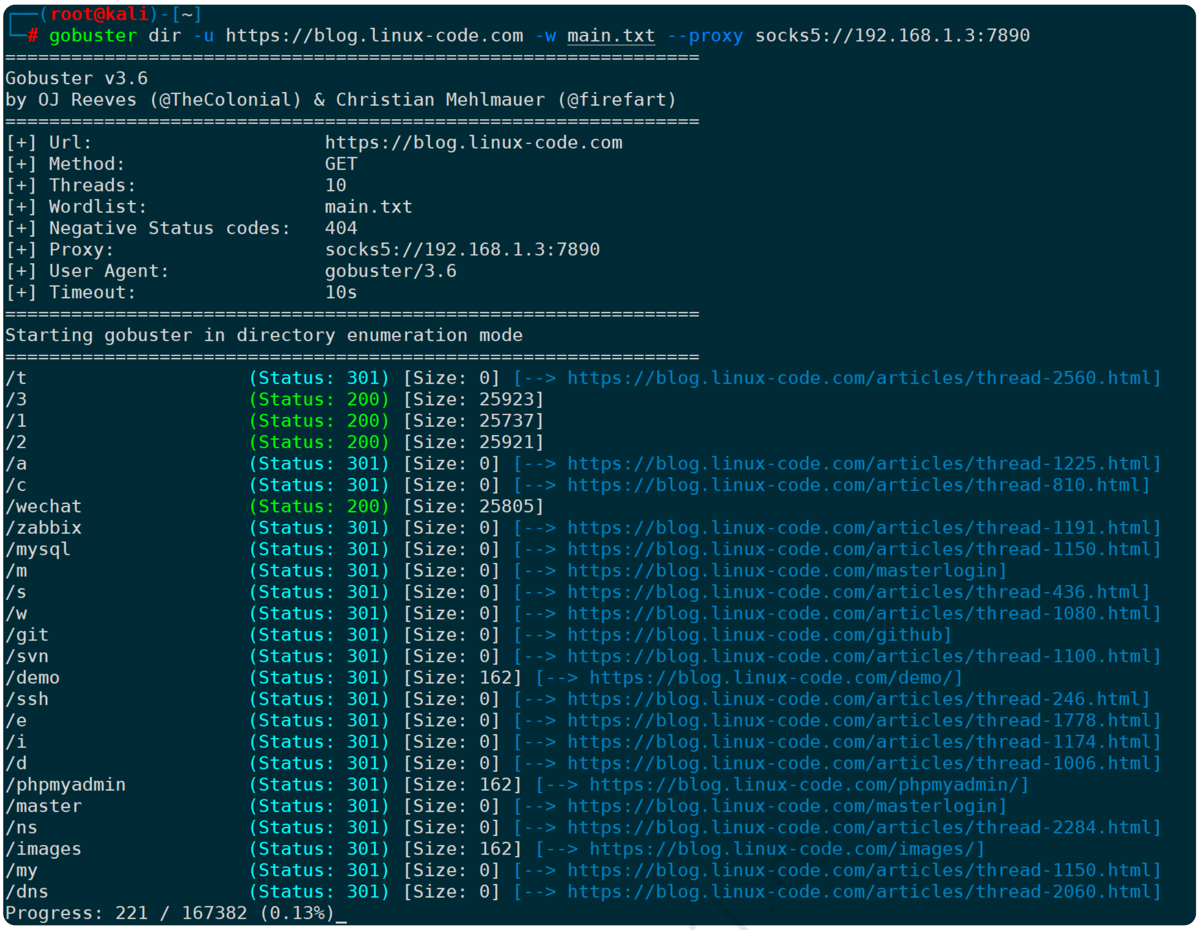
10.指定代理服务器（--proxy）

不想暴露真实IP的情况，可以指定代理选项，支持HTTP/HTTPS代理，或者socks5代理。

格式为：[http(s)://host:port] 或者 [socks5://host:port]

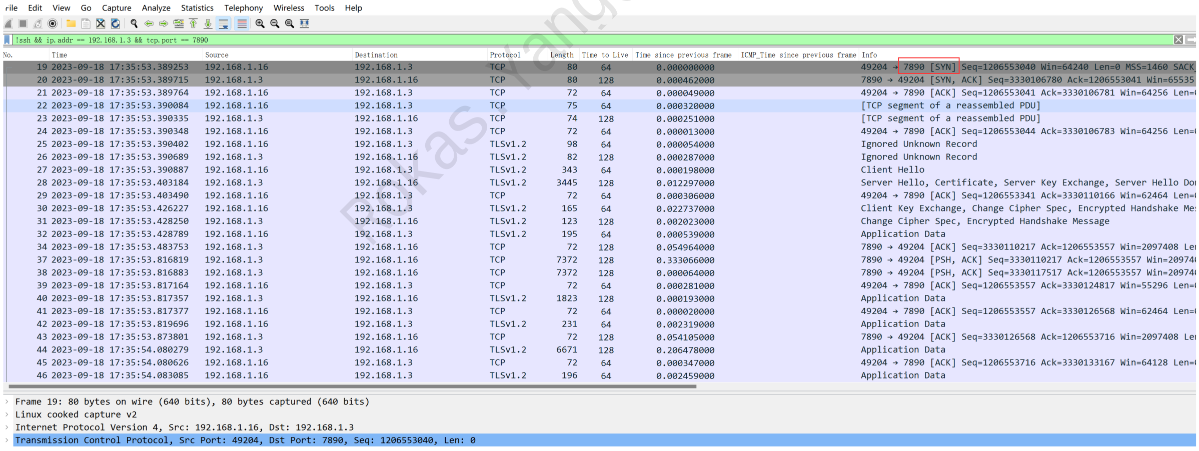
比如指定socks5代理来扫描对方，可以是：

```
gobuster dir -u <URL> -w <wordlist> --proxy <socks5://host:port>
```



```
┌──(root㉿kali)-[~]
└─# gobuster dir -u https://blog.linux-code.com -w main.txt --proxy socks5://192.168.1.3:7890
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://blog.linux-code.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                main.txt
[+] Negative Status codes:   404
[+] Proxy:                   socks5://192.168.1.3:7890
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/t                    (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-2560.html]
/3                    (Status: 200) [Size: 25923]
/1                    (Status: 200) [Size: 25737]
/2                    (Status: 200) [Size: 25921]
/a                    (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-1225.html]
/c                    (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-810.html]
/wechat               (Status: 200) [Size: 25805]
/zabbix               (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-1191.html]
/mysql                (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-1150.html]
/m                    (Status: 301) [Size: 0] [--> https://blog.linux-code.com/masterlogin]
/s                    (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-436.html]
/w                    (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-1080.html]
/git                  (Status: 301) [Size: 0] [--> https://blog.linux-code.com/github]
/svn                  (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-1100.html]
/demo                 (Status: 301) [Size: 162] [--> https://blog.linux-code.com/demo/]
/ssh                  (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-246.html]
/e                    (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-1778.html]
/i                    (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-1174.html]
/d                    (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-1006.html]
/phpmyadmin           (Status: 301) [Size: 162] [--> https://blog.linux-code.com/phpmyadmin/]
/master               (Status: 301) [Size: 0] [--> https://blog.linux-code.com/masterlogin]
/ns                   (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-2284.html]
/images               (Status: 301) [Size: 162] [--> https://blog.linux-code.com/images/]
/my                   (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-1150.html]
/dns                  (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-2060.html]
Progress: 221 / 167382 (0.13%)_
```

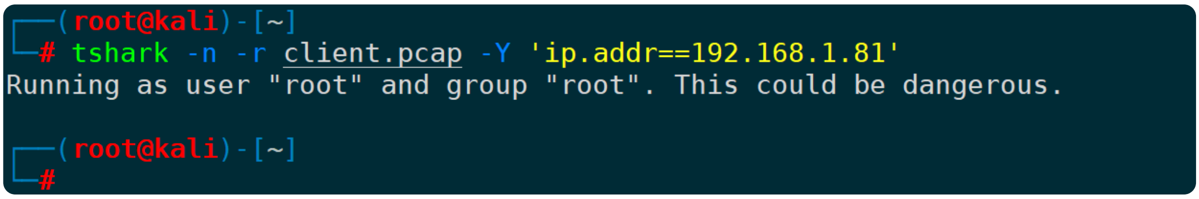
通过在kali客户端抓包发现，客户端将请求转发给设置的代理伺服器，让它来完成整个扫描：



```
!ssh && ip.addr == 192.168.1.3 && tcp.port == 7890

No.  Time                        Source        Destination   Protocol Length Time to Live Time since previous frame ICMP_Time since previous frame Info
  19 2023-09-18 17:35:53.389253  192.168.1.16  192.168.1.3   TCP        80    64   0.000000000   49204 → 7890 [SYN] Seq=1206553040 Win=64240 Len=0 MSS=1460 SACK_
  20 2023-09-18 17:35:53.389715  192.168.1.3   192.168.1.16  TCP        80   128   0.000462000   7890 → 49204 [SYN, ACK] Seq=3330106780 Ack=1206553041 Win=65535
  21 2023-09-18 17:35:53.389764  192.168.1.16  192.168.1.3   TCP        72    64   0.000049000   49204 → 7890 [ACK] Seq=1206553041 Ack=3330106781 Win=64256 Len=
  22 2023-09-18 17:35:53.390084  192.168.1.16  192.168.1.3   TCP        75    64   0.000320000   [TCP segment of a reassembled PDU]
  23 2023-09-18 17:35:53.390335  192.168.1.3   192.168.1.16  TCP        74   128   0.000251000   [TCP segment of a reassembled PDU]
  24 2023-09-18 17:35:53.390348  192.168.1.16  192.168.1.3   TCP        72    64   0.000013000   49204 → 7890 [ACK] Seq=1206553044 Ack=3330106783 Win=64256 Len=
  25 2023-09-18 17:35:53.390402  192.168.1.16  192.168.1.3   TLSv1.2    98    64   0.000054000   Ignored Unknown Record
  26 2023-09-18 17:35:53.390689  192.168.1.3   192.168.1.16  TLSv1.2    82   128   0.000287000   Ignored Unknown Record
  27 2023-09-18 17:35:53.390887  192.168.1.16  192.168.1.3   TLSv1.2   343    64   0.000198000   Client Hello
  28 2023-09-18 17:35:53.403184  192.168.1.3   192.168.1.16  TLSv1.2  3445   128   0.012297000   Server Hello, Certificate, Server Key Exchange, Server Hello Do
  29 2023-09-18 17:35:53.403490  192.168.1.16  192.168.1.3   TCP        72    64   0.000306000   49204 → 7890 [ACK] Seq=1206553341 Ack=3330110166 Win=62464 Len=
  30 2023-09-18 17:35:53.426227  192.168.1.16  192.168.1.3   TLSv1.2   165    64   0.022737000   Client Key Exchange, Change Cipher Spec, Encrypted Handshake Me
  31 2023-09-18 17:35:53.428250  192.168.1.3   192.168.1.16  TLSv1.2   123   128   0.002023000   Change Cipher Spec, Encrypted Handshake Message
  32 2023-09-18 17:35:53.428789  192.168.1.16  192.168.1.3   TLSv1.2   195    64   0.000539000   Application Data
  34 2023-09-18 17:35:53.483753  192.168.1.3   192.168.1.16  TCP        72   128   0.054964000   7890 → 49204 [ACK] Seq=3330110217 Ack=1206553557 Win=2097408 Le
  37 2023-09-18 17:35:53.816819  192.168.1.3   192.168.1.16  TCP      7372   128   0.333066000   7890 → 49204 [PSH, ACK] Seq=3330110217 Ack=1206553557 Win=20974
  38 2023-09-18 17:35:53.816883  192.168.1.3   192.168.1.16  TCP      7372   128   0.000064000   7890 → 49204 [PSH, ACK] Seq=3330117517 Ack=1206553557 Win=20974
  39 2023-09-18 17:35:53.817164  192.168.1.16  192.168.1.3   TCP        72    64   0.000281000   49204 → 7890 [ACK] Seq=1206553557 Ack=3330124817 Win=55296 Len=
  40 2023-09-18 17:35:53.817357  192.168.1.3   192.168.1.16  TLSv1.2  1823   128   0.000193000   Application Data
  41 2023-09-18 17:35:53.817377  192.168.1.16  192.168.1.3   TCP        72    64   0.000020000   49204 → 7890 [ACK] Seq=1206553557 Ack=3330126568 Win=62464 Len=
  42 2023-09-18 17:35:53.819696  192.168.1.16  192.168.1.3   TLSv1.2   231    64   0.002319000   Application Data
  43 2023-09-18 17:35:53.873801  192.168.1.3   192.168.1.16  TCP        72   128   0.054105000   7890 → 49204 [ACK] Seq=3330126568 Ack=1206553716 Win=2097408 Le
  44 2023-09-18 17:35:54.080279  192.168.1.3   192.168.1.16  TLSv1.2  6671   128   0.206478000   Application Data
  45 2023-09-18 17:35:54.080626  192.168.1.16  192.168.1.3   TCP        72    64   0.000347000   49204 → 7890 [ACK] Seq=1206553716 Ack=3330133167 Win=64128 Len=
  46 2023-09-18 17:35:54.083085  192.168.1.16  192.168.1.3   TLSv1.2   196    64   0.002459000   Application Data

> Frame 19: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
> Linux cooked capture v2
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.3
> Transmission Control Protocol, Src Port: 49204, Dst Port: 7890, Seq: 1206553040, Len: 0
```

因为整个过程是加密了，所以不能直接看出请求的内容。

但不难发现整个过程客户端本身并不会去直接请求被扫描的目的服务器：



```
┌──(root㉿kali)-[~]
└─# tshark -n -r client.pcap -Y 'ip.addr==192.168.1.81'
Running as user "root" and group "root". This could be dangerous.

┌──(root㉿kali)-[~]
└─#
```

11.指定客户端证书及私钥（--client-cert-[p12|pem]）

在TLS/SSL双向认证的场景下，客户端请求服务端需要指定客户端证书的，则可以使用此参数指定。

指定p12证书为：

```
gobuster dir --client-cert-p12 <certfile> -w <wordlist> -u <URL>
```

如果p12证书有密码：

```
gobuster dir --client-cert-p12 <certfile> --client-cert-p12-password
<certpasswordfile> -w <wordlist> -u <URL>
```

同理，指定pem证书则为：

```
gobuster dir --client-cert-pem <certfile> -w <wordlist> -u <URL>
```

如果有pem证书的私钥：

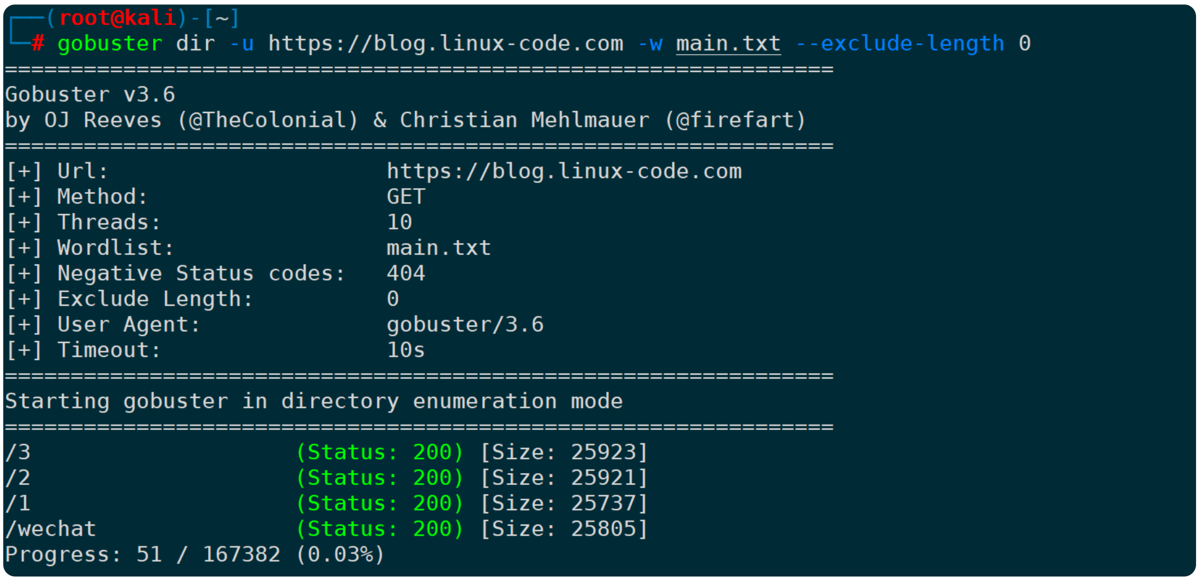
```
gobuster dir --client-cert-pem <certfile> --client-cert-pem-key <keyfile> -w
<wordlist> -u <URL>
```

12.剔除指定内容长度的结果（--exclude-length）

当对返回的结果内容长度有要求时，可以通过此参数指定。

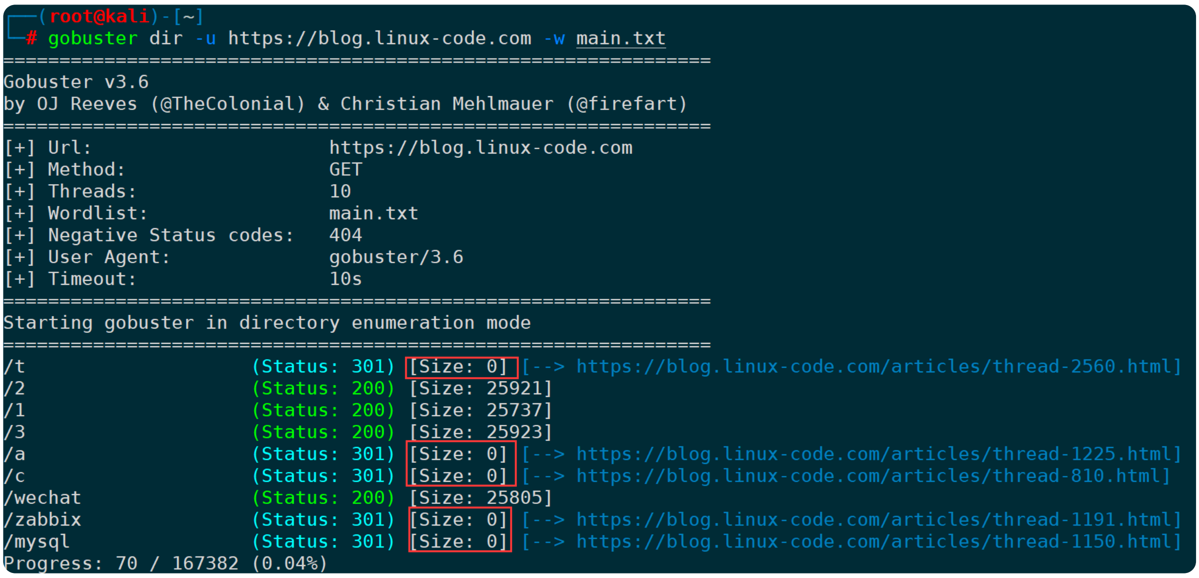
比如，剔除内容长度为0字节的情况：

```
gobuster dir -u <URL> -w <wordlist> --exclude-length 0
```



```
┌──(root@kali)-[~]
└─# gobuster dir -u https://blog.linux-code.com -w main.txt --exclude-length 0
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://blog.linux-code.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                main.txt
[+] Negative Status codes:   404
[+] Exclude Length:          0
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/3                    (Status: 200) [Size: 25923]
/2                    (Status: 200) [Size: 25921]
/1                    (Status: 200) [Size: 25737]
/wechat               (Status: 200) [Size: 25805]
Progress: 51 / 167382 (0.03%)
```

再看看不指定的效果：

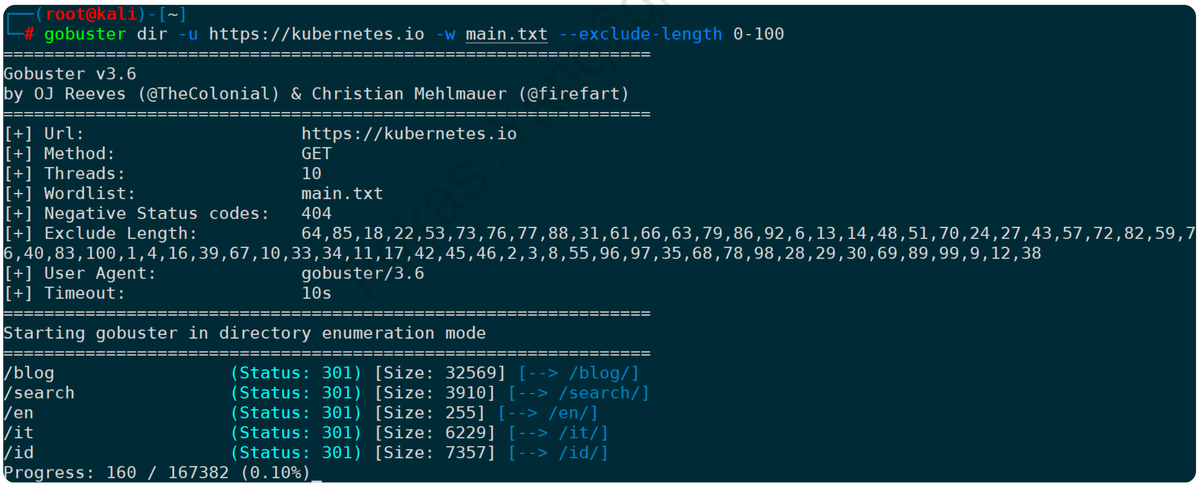


```
┌──(root@kali)-[~]
└─# gobuster dir -u https://blog.linux-code.com -w main.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://blog.linux-code.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                main.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/t                    (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-2560.html]
/2                    (Status: 200) [Size: 25921]
/1                    (Status: 200) [Size: 25737]
/3                    (Status: 200) [Size: 25923]
/a                    (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-1225.html]
/c                    (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-810.html]
/wechat               (Status: 200) [Size: 25805]
/zabbix               (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-1191.html]
/mysql                (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-1150.html]
Progress: 70 / 167382 (0.04%)
```

很明显返回了很多字节为0的页面，基本都为301重定向，并显示了重定向后的URL地址。

如果想剔除在某个大小范围内的结果，通过-字符来指定，比如剔除介于**0-100**字节大小的结果：

```
gobuster dir -u <URL> -w <wordlist> --exclude-length 0-100
```



```
┌──(root@kali)-[~]
└─# gobuster dir -u https://kubernetes.io -w main.txt --exclude-length 0-100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://kubernetes.io
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                main.txt
[+] Negative Status codes:   404
[+] Exclude Length:          64,85,18,22,53,73,76,77,88,31,61,66,63,79,86,92,6,13,14,48,51,70,24,27,43,57,72,82,59,7
6,40,83,100,1,4,16,39,67,10,33,34,11,17,42,45,46,2,3,8,55,96,97,35,68,78,98,28,29,30,69,89,99,9,12,38
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/blog                 (Status: 301) [Size: 32569] [--> /blog/]
/search               (Status: 301) [Size: 3910] [--> /search/]
/en                   (Status: 301) [Size: 255] [--> /en/]
/it                   (Status: 301) [Size: 6229] [--> /it/]
/id                   (Status: 301) [Size: 7357] [--> /id/]
Progress: 160 / 167382 (0.10%)_
```

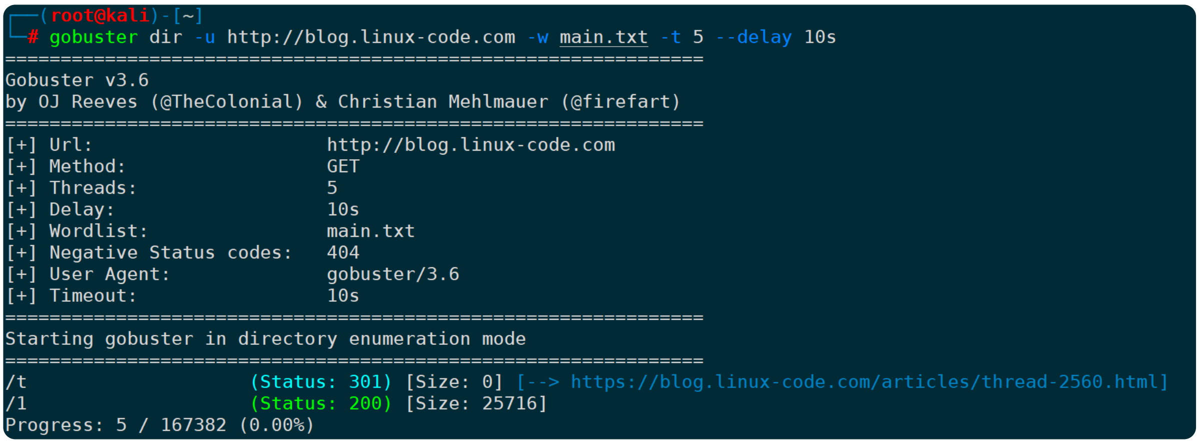
13.指定线程数和延时时间（-t|--delay）

这两个参数都属于全局参数，并非**dir模式**独有，但组合在一起用值得单独拎出来讲一下。

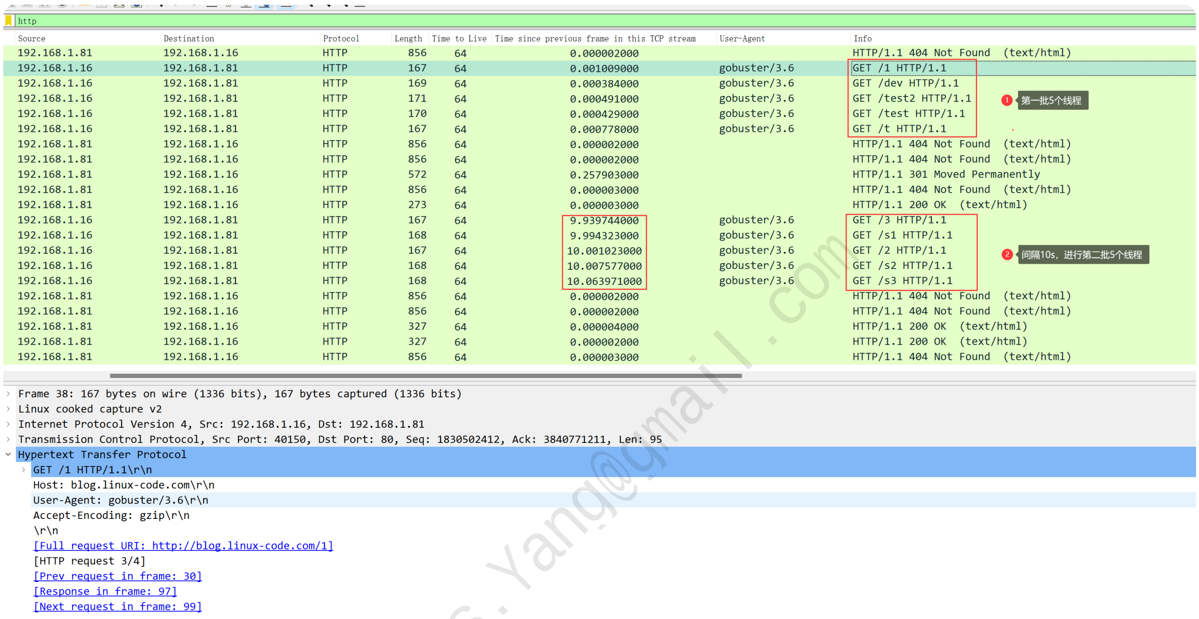
如果对端服务器有做QPS限频处理，那么触发阈值则可能全部超时或者拿到不符合预期的状态码，可以通过指定线程数和延时时间来将动作放慢，默认不指定的情况，**-t**每次10个线程，且没有delay时间。

比如每次执行5个线程，然后延时10s再继续下5个线程：

```
gobuster dir -u <URL> -w <wordlist> -t 5 --delay 10s
```



```
┌──(root@kali)-[~]
└─# gobuster dir -u http://blog.linux-code.com -w main.txt -t 5 --delay 10s
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://blog.linux-code.com
[+] Method:                  GET
[+] Threads:                 5
[+] Delay:                   10s
[+] Wordlist:                main.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/t                    (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-2560.html]
/1                    (Status: 200) [Size: 25716]
Progress: 5 / 167382 (0.00%)
```



http

Source	Destination	Protocol	Length	Time to Live	Time since previous frame in this TCP stream	User-Agent	Info
192.168.1.81	192.168.1.16	HTTP	856	64	0.000002000		HTTP/1.1 404 Not Found (text/html)
192.168.1.16	192.168.1.81	HTTP	167	64	0.001009000	gobuster/3.6	GET /1 HTTP/1.1
192.168.1.16	192.168.1.81	HTTP	169	64	0.000384000	gobuster/3.6	GET /dev HTTP/1.1
192.168.1.16	192.168.1.81	HTTP	171	64	0.000491000	gobuster/3.6	GET /test2 HTTP/1.1
192.168.1.16	192.168.1.81	HTTP	170	64	0.000429000	gobuster/3.6	GET /test HTTP/1.1
192.168.1.16	192.168.1.81	HTTP	167	64	0.000778000	gobuster/3.6	GET /t HTTP/1.1
192.168.1.81	192.168.1.16	HTTP	856	64	0.000002000		HTTP/1.1 404 Not Found (text/html)
192.168.1.81	192.168.1.16	HTTP	856	64	0.000002000		HTTP/1.1 404 Not Found (text/html)
192.168.1.81	192.168.1.16	HTTP	572	64	0.257903000		HTTP/1.1 301 Moved Permanently
192.168.1.81	192.168.1.16	HTTP	856	64	0.000003000		HTTP/1.1 404 Not Found (text/html)
192.168.1.81	192.168.1.16	HTTP	273	64	0.000003000		HTTP/1.1 200 OK (text/html)
192.168.1.16	192.168.1.81	HTTP	167	64	9.939744000	gobuster/3.6	GET /3 HTTP/1.1
192.168.1.16	192.168.1.81	HTTP	168	64	9.994323000	gobuster/3.6	GET /s1 HTTP/1.1
192.168.1.16	192.168.1.81	HTTP	167	64	10.001023000	gobuster/3.6	GET /2 HTTP/1.1
192.168.1.16	192.168.1.81	HTTP	168	64	10.007577000	gobuster/3.6	GET /s2 HTTP/1.1
192.168.1.16	192.168.1.81	HTTP	168	64	10.063971000	gobuster/3.6	GET /s3 HTTP/1.1
192.168.1.81	192.168.1.16	HTTP	856	64	0.000002000		HTTP/1.1 404 Not Found (text/html)
192.168.1.81	192.168.1.16	HTTP	856	64	0.000002000		HTTP/1.1 404 Not Found (text/html)
192.168.1.81	192.168.1.16	HTTP	327	64	0.000004000		HTTP/1.1 200 OK (text/html)
192.168.1.81	192.168.1.16	HTTP	327	64	0.000002000		HTTP/1.1 200 OK (text/html)
192.168.1.81	192.168.1.16	HTTP	856	64	0.000003000		HTTP/1.1 404 Not Found (text/html)

1 第一批5个线程

2 间隔10s，进行第二批5个线程

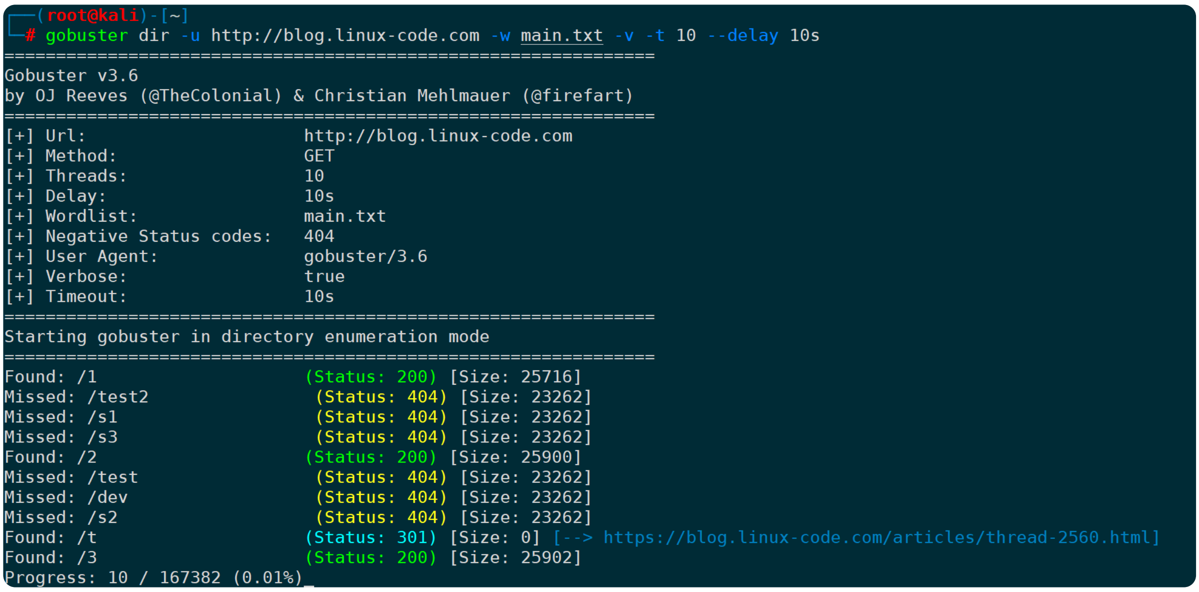
```
> Frame 38: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits)
> Linux cooked capture v2
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.81
> Transmission Control Protocol, Src Port: 40150, Dst Port: 80, Seq: 1830502412, Ack: 3840771211, Len: 95
v Hypertext Transfer Protocol
  > GET /1 HTTP/1.1\r\n
    Host: blog.linux-code.com\r\n
    User-Agent: gobuster/3.6\r\n
    Accept-Encoding: gzip\r\n
    \r\n
    [Full request URI: http://blog.linux-code.com/1]
    [HTTP request 3/4]
    [Prev request in frame: 30]
    [Response in frame: 97]
    [Next request in frame: 99]
```

14.设置黑名单状态码（-b|--status-codes-blacklist）

默认情况下，此参数值为404，即通过字典枚举构造的URL，请求过去如果拿到的是404状态码，则不展示在结果上，因此上面的所有gobuster执行截图，没有看到任何404状态码的结果。

而如果你想看到执行过程，哪怕404页面也要返回的话，全局模式的-v参数可以详细打印日志：

```
gobuster dir -u <URL> -w <wordlist> -v
```

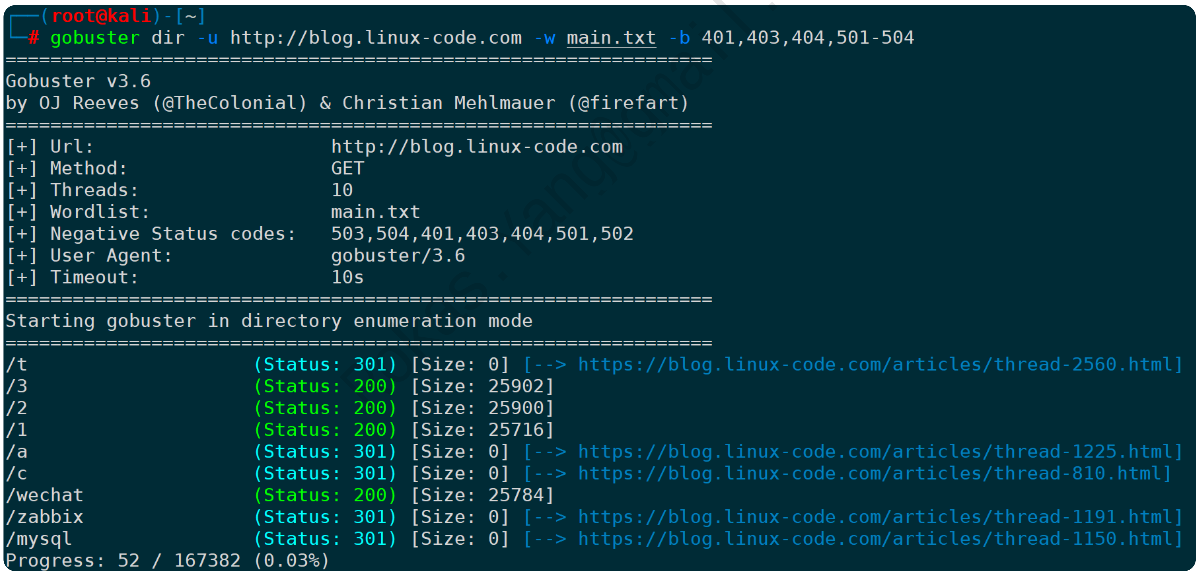


```
┌──(root@kali)-[~]
└─# gobuster dir -u http://blog.linux-code.com -w main.txt -v -t 10 --delay 10s
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://blog.linux-code.com
[+] Method:                  GET
[+] Threads:                 10
[+] Delay:                   10s
[+] Wordlist:                main.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Verbose:                 true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
Found: /1                    (Status: 200) [Size: 25716]
Missed: /test2                (Status: 404) [Size: 23262]
Missed: /s1                   (Status: 404) [Size: 23262]
Missed: /s3                   (Status: 404) [Size: 23262]
Found: /2                    (Status: 200) [Size: 25900]
Missed: /test                 (Status: 404) [Size: 23262]
Missed: /dev                  (Status: 404) [Size: 23262]
Missed: /s2                   (Status: 404) [Size: 23262]
Found: /t                    (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-2560.html]
Found: /3                    (Status: 200) [Size: 25902]
Progress: 10 / 167382 (0.01%)
```

可以看到404页面会在最前面标记为Missed。

-b参数可以设置哪些HTTP状态码不展示到结果上，比如401、403、404、501-504都不展示，可以是：

```
gobuster dir -u <URL> -w <wordlist> -b 401,403,404,501-504
```

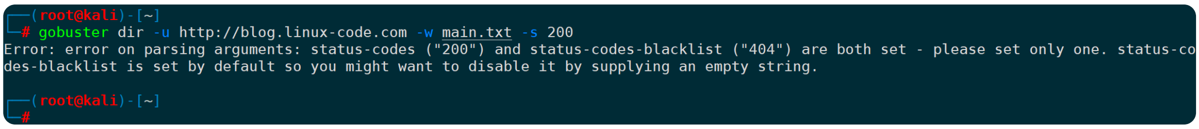


```
┌──(root@kali)-[~]
└─# gobuster dir -u http://blog.linux-code.com -w main.txt -b 401,403,404,501-504
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://blog.linux-code.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                main.txt
[+] Negative Status codes:   503,504,401,403,404,501,502
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/t                    (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-2560.html]
/3                    (Status: 200) [Size: 25902]
/2                    (Status: 200) [Size: 25900]
/1                    (Status: 200) [Size: 25716]
/a                    (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-1225.html]
/c                    (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-810.html]
/wechat               (Status: 200) [Size: 25784]
/zabbix               (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-1191.html]
/mysql                (Status: 301) [Size: 0] [--> https://blog.linux-code.com/articles/thread-1150.html]
Progress: 52 / 167382 (0.03%)
```

15.筛选指定状态码（-s|--status-codes）

同理，有黑名单就有白名单，此参数用来指定符合条件的状态码。

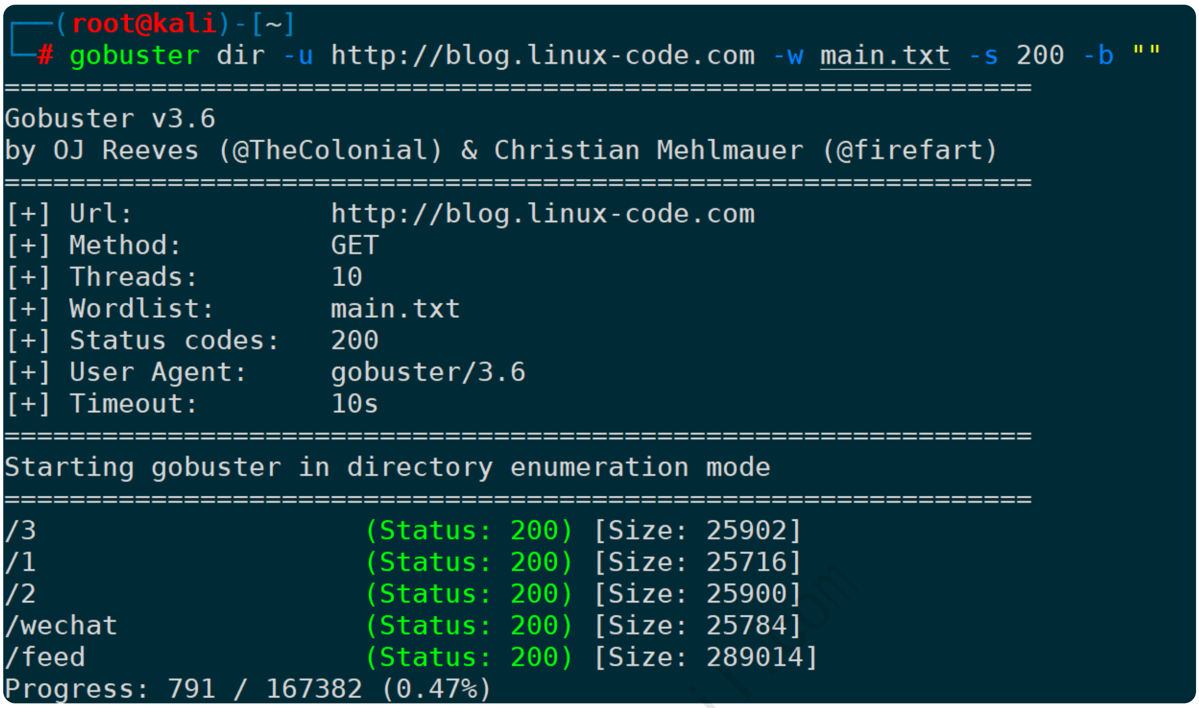
-s和-b互斥，不能同时设置（缺省情况下-b为404），因此使用-s时，-b必须要设置为空字符串（`-b ""`），不然会报错：**Error: error on parsing arguments: status-codes ("200") and status-codes-blacklist ("404") are both set - please set only one. status-codes-blacklist is set by default so you might want to disable it by supplying an empty string.**



```
┌──(root@kali)-[~]
└─# gobuster dir -u http://blog.linux-code.com -w main.txt -s 200
Error: error on parsing arguments: status-codes ("200") and status-codes-blacklist ("404") are both set - please set only one. status-co
des-blacklist is set by default so you might want to disable it by supplying an empty string.

┌──(root@kali)-[~]
└─#
```

因此，只想要200状态码的结果，可以写成：

```
gobuster dir -u <URL> -w <wordlist> -s 200 -b ""
```



```
┌──(root@kali)-[~]
└─# gobuster dir -u http://blog.linux-code.com -w main.txt -s 200 -b ""
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://blog.linux-code.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                main.txt
[+] Status codes:            200
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/3                    (Status: 200) [Size: 25902]
/1                    (Status: 200) [Size: 25716]
/2                    (Status: 200) [Size: 25900]
/wechat               (Status: 200) [Size: 25784]
/feed                 (Status: 200) [Size: 289014]
Progress: 791 / 167382 (0.47%)
```

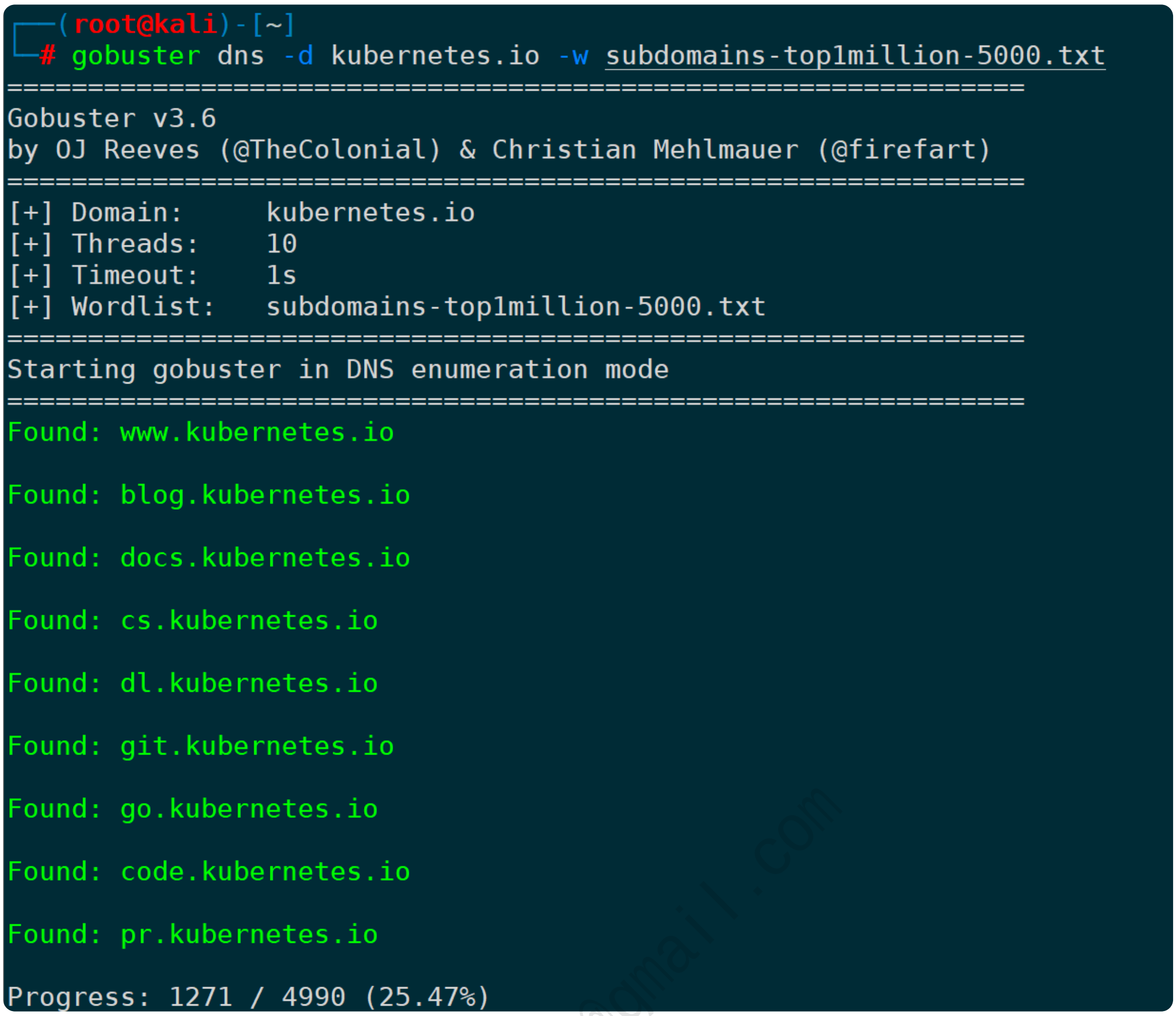
> 当然也可以同时指定多个或者范围，如：`-s 200,300-399,401 -b ""`

五、DNS子域名暴力枚举（dns）

1.指定域名枚举（-d|--domain）

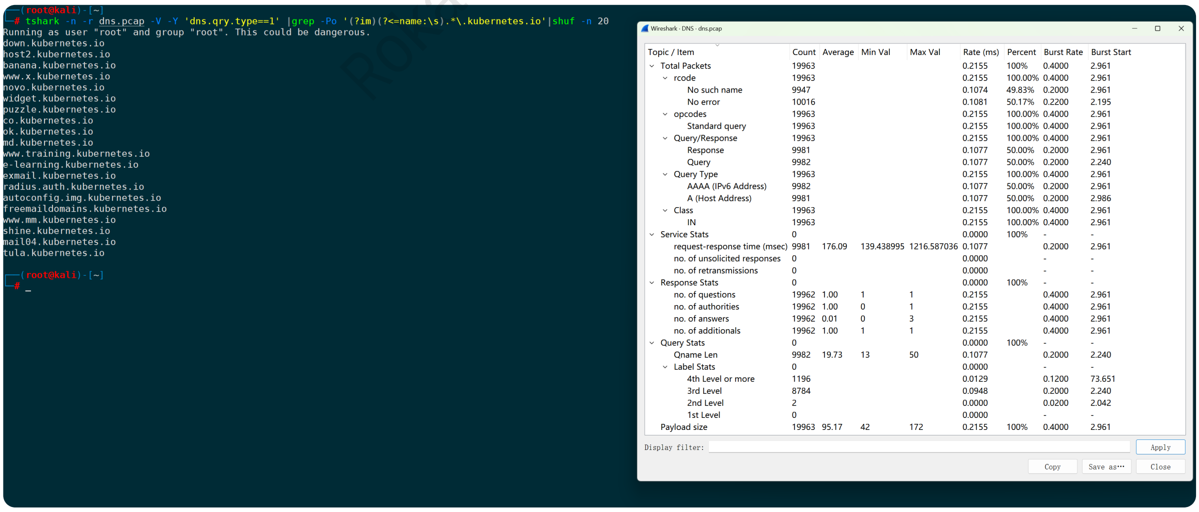
-d参数指定目标域名，**-w**指定字典，以k8s官网为例：

```
gobuster -d kubernetes.io -w <wordlist>
```



```
┌──(root@kali)-[~]
└─# gobuster dns -d kubernetes.io -w subdomains-top1million-5000.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     kubernetes.io
[+] Threads:    10
[+] Timeout:    1s
[+] Wordlist:   subdomains-top1million-5000.txt
===============================================================
Starting gobuster in DNS enumeration mode
===============================================================
Found: www.kubernetes.io

Found: blog.kubernetes.io

Found: docs.kubernetes.io

Found: cs.kubernetes.io

Found: dl.kubernetes.io

Found: git.kubernetes.io

Found: go.kubernetes.io

Found: code.kubernetes.io

Found: pr.kubernetes.io

Progress: 1271 / 4990 (25.47%)
```

通过抓包可以看到，gobuster将字典里面的条目，填充到指定的域名形成子域名，并一次次向DNS服务器发起query请求进行DNS穷举：



```
┌──(root@kali)-[~]
└─# tshark -n -r dns.pcap -V -Y 'dns.qry.type==1' |grep -Po '(?im)(?<=name:\s).*\.kubernetes.io'|shuf -n 20
Running as user "root" and group "root". This could be dangerous.
down.kubernetes.io
host2.kubernetes.io
banana.kubernetes.io
www.x.kubernetes.io
novo.kubernetes.io
widget.kubernetes.io
puzzle.kubernetes.io
co.kubernetes.io
ok.kubernetes.io
md.kubernetes.io
www.training.kubernetes.io
e-learning.kubernetes.io
exmail.kubernetes.io
radius.auth.kubernetes.io
autoconfig.img.kubernetes.io
freemaildomains.kubernetes.io
www.mm.kubernetes.io
shine.kubernetes.io
mail04.kubernetes.io
tula.kubernetes.io

┌──(root@kali)-[~]
└─# _
```

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total Packets	19963				0.2155	100%	0.4000	2.961
rcode	19963				0.2155	100.00%	0.4000	2.961
No such name	9947				0.1074	49.83%	0.2000	2.961
No error	10016				0.1081	50.17%	0.2200	2.195
opcodes	19963				0.2155	100.00%	0.4000	2.961
Standard query	19963				0.2155	100.00%	0.4000	2.961
Query/Response	19963				0.2155	100.00%	0.4000	2.961
Response	9981				0.1077	50.00%	0.2000	2.961
Query	9982				0.1077	50.00%	0.2000	2.240
Query Type	19963				0.2155	100.00%	0.4000	2.961
AAAA (IPv6 Address)	9982				0.1077	50.00%	0.2000	2.961
A (Host Address)	9981				0.1077	50.00%	0.2000	2.986
Class	19963				0.2155	100.00%	0.4000	2.961
IN	19963				0.2155	100.00%	0.4000	2.961
Service Stats	0				0.0000	100%	-	-
request-response time (msec)	9981	176.09	139.438995	1216.587036	0.1077		0.2000	2.961
no. of unsolicited responses	0				0.0000		-	-
no. of retransmissions	0				0.0000		-	-
Response Stats	0				0.0000	100%	-	-
no. of questions	19962	1.00	1	1	0.2155		0.4000	2.961
no. of authorities	19962	1.00	0	1	0.2155		0.4000	2.961
no. of answers	19962	0.01	0	3	0.2155		0.4000	2.961
no. of additionals	19962	1.00	1	1	0.2155		0.4000	2.961
Query Stats	0				0.0000	100%	-	-
Qname Len	9982	19.73	13	50	0.1077		0.2000	2.240
Label Stats	0				0.0000		-	-
4th Level or more	1196				0.0129		0.1200	73.651
3rd Level	8784				0.0948		0.2000	2.240
2nd Level	2				0.0000		0.0200	2.042
1st Level	0				0.0000		-	-
Payload size	19963	95.17	42	172	0.2155	100%	0.4000	2.961

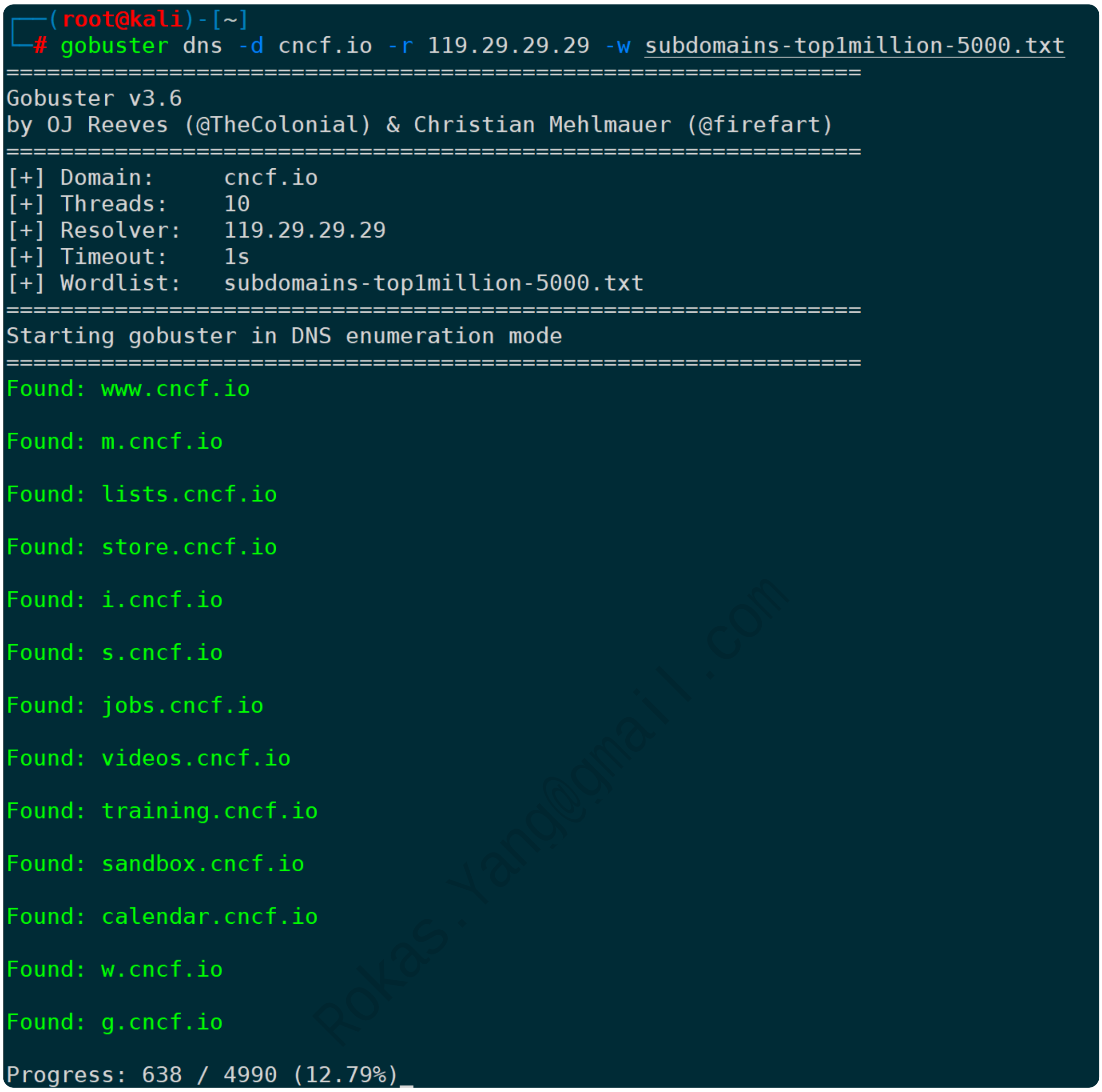
Display filter:

2.指定DNS服务器解析（-r|--resolver）

如果不想走系统配置的默认DNS，也不想修改系统的DNS配置，那么-r可以任意指定DNS服务器进行解析：

比如指定腾讯云的公共DNS：119.29.29.29 来枚举CNCF的子域名：

```
gobuster dns -d cncf.io -r 119.29.29.29 -w <wordlist>
```

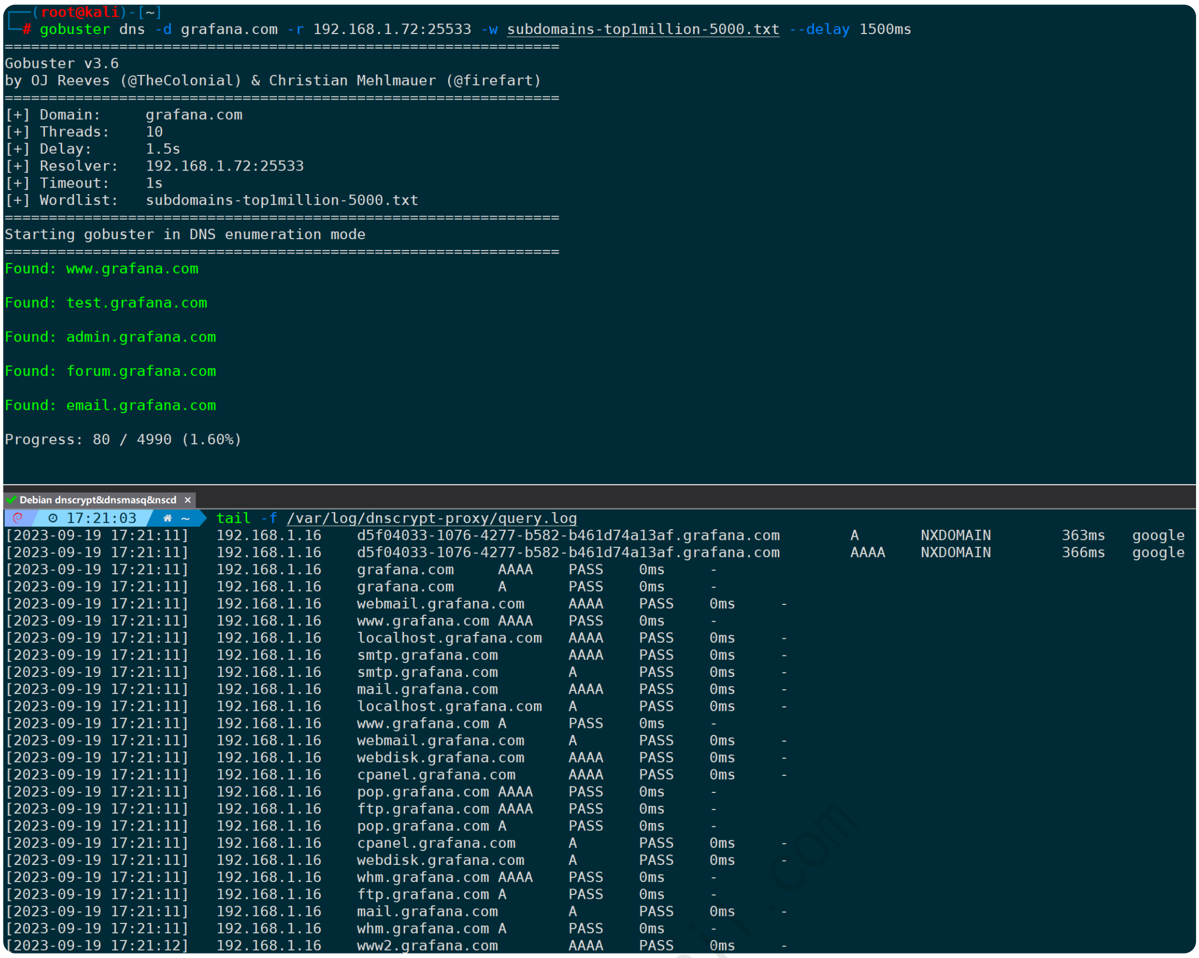


```
┌──(root@kali)-[~]
└─# gobuster dns -d cncf.io -r 119.29.29.29 -w subdomains-top1million-5000.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     cncf.io
[+] Threads:    10
[+] Resolver:   119.29.29.29
[+] Timeout:    1s
[+] Wordlist:   subdomains-top1million-5000.txt
===============================================================
Starting gobuster in DNS enumeration mode
===============================================================
Found: www.cncf.io

Found: m.cncf.io

Found: lists.cncf.io

Found: store.cncf.io

Found: i.cncf.io

Found: s.cncf.io

Found: jobs.cncf.io

Found: videos.cncf.io

Found: training.cncf.io

Found: sandbox.cncf.io

Found: calendar.cncf.io

Found: w.cncf.io

Found: g.cncf.io

Progress: 638 / 4990 (12.79%)_
```

默认去请求DNS服务器53端口，如果是非默认的其它端口，指定端口即可。

比如请求内网DNS的高端口25533枚举grafana官网的子域名，并且指定每个线程延时时间为1.5s：

```
gobuster dns -d grafana.com -r 192.168.1.72:25533 -w <wordlist> --delay 1500ms
```



```
┌──(root㉿kali)-[~]
└─# gobuster dns -d grafana.com -r 192.168.1.72:25533 -w subdomains-top1million-5000.txt --delay 1500ms
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     grafana.com
[+] Threads:    10
[+] Delay:      1.5s
[+] Resolver:   192.168.1.72:25533
[+] Timeout:    1s
[+] Wordlist:   subdomains-top1million-5000.txt
===============================================================
Starting gobuster in DNS enumeration mode
===============================================================
Found: www.grafana.com

Found: test.grafana.com

Found: admin.grafana.com

Found: forum.grafana.com

Found: email.grafana.com

Progress: 80 / 4990 (1.60%)
```

```
 17:21:03   ~  tail -f /var/log/dnscrypt-proxy/query.log
[2023-09-19 17:21:11]   192.168.1.16    d5f04033-1076-4277-b582-b461d74a13af.grafana.com        A       NXDOMAIN        363ms   google
[2023-09-19 17:21:11]   192.168.1.16    d5f04033-1076-4277-b582-b461d74a13af.grafana.com        AAAA    NXDOMAIN        366ms   google
[2023-09-19 17:21:11]   192.168.1.16    grafana.com     AAAA    PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    grafana.com     A       PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    webmail.grafana.com     AAAA    PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    www.grafana.com AAAA    PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    localhost.grafana.com   AAAA    PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    smtp.grafana.com        AAAA    PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    smtp.grafana.com        A       PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    mail.grafana.com        AAAA    PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    localhost.grafana.com   A       PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    www.grafana.com A       PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    webmail.grafana.com     A       PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    webdisk.grafana.com     AAAA    PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    cpanel.grafana.com      AAAA    PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    pop.grafana.com AAAA    PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    ftp.grafana.com AAAA    PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    pop.grafana.com A       PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    cpanel.grafana.com      A       PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    webdisk.grafana.com     A       PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    whm.grafana.com AAAA    PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    ftp.grafana.com A       PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    mail.grafana.com        A       PASS    0ms     -
[2023-09-19 17:21:11]   192.168.1.16    whm.grafana.com A       PASS    0ms     -
[2023-09-19 17:21:12]   192.168.1.16    www2.grafana.com        AAAA    PASS    0ms     -
```

3.打印cname记录（-c|--show-cname）

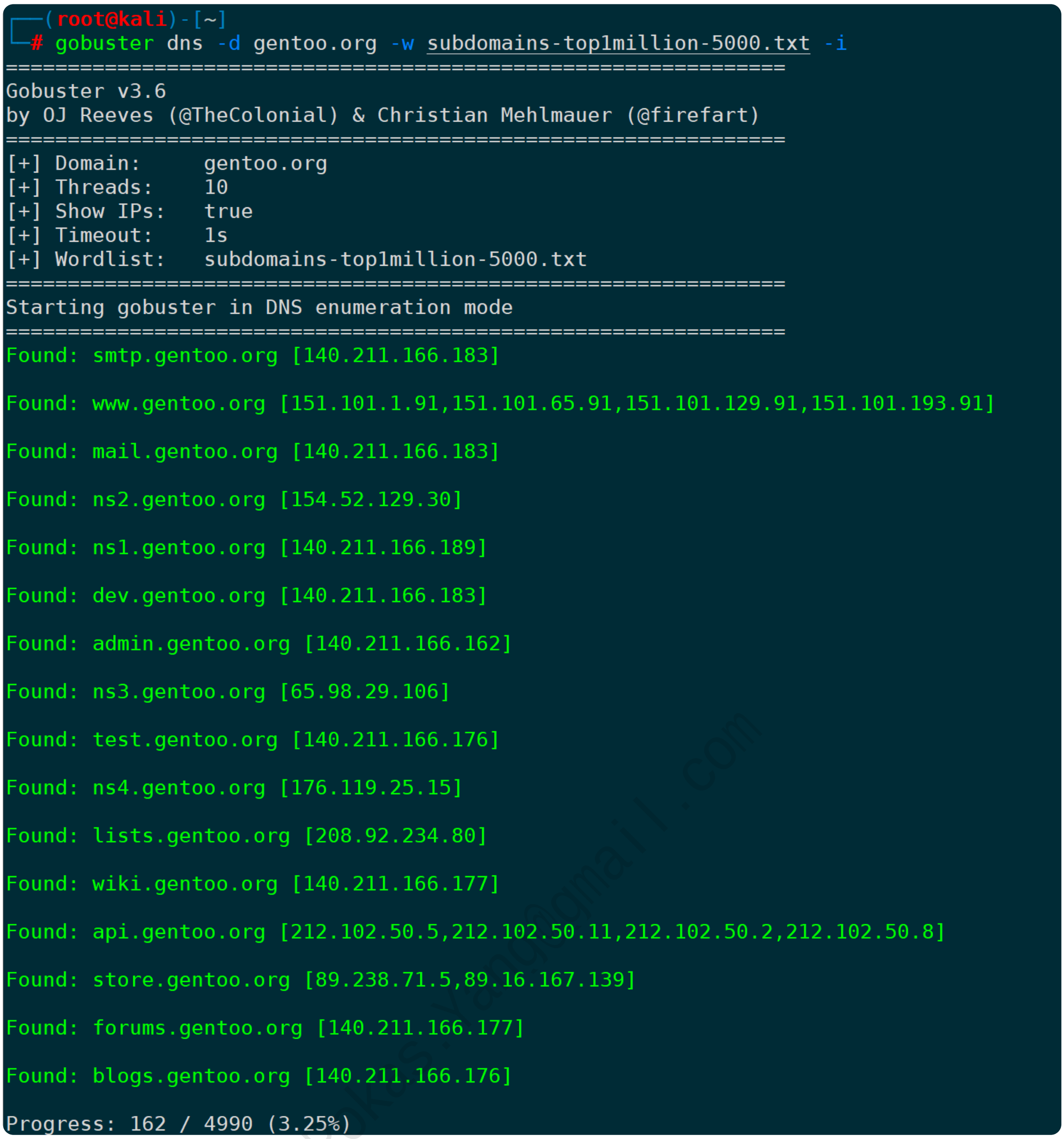
想要输出别名记录时，则可以使用-c参数：

```
gobuster dns -c -d <domain> -w <wordlist>
```

4.打印解析到的IP（-i|--show-ips）

想要知道每个枚举出来的域名对应的解析记录时，可使用-i参数，以枚举gentoo官网为例：

```
gobuster dns -d gentoo.org -w <wordlist> -i
```

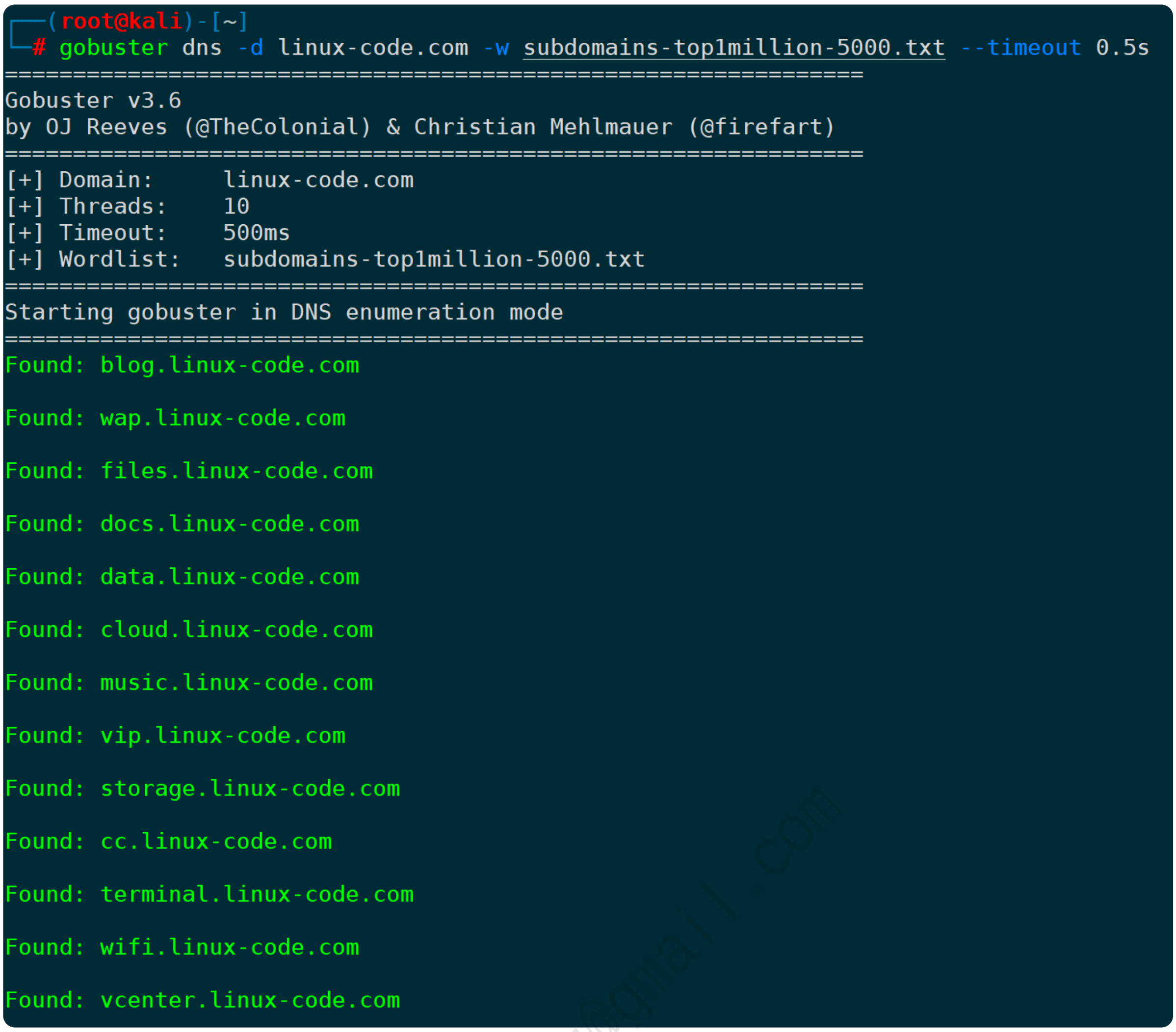


```
┌──(root@kali)-[~]
└─# gobuster dns -d gentoo.org -w subdomains-top1million-5000.txt -i
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     gentoo.org
[+] Threads:    10
[+] Show IPs:   true
[+] Timeout:    1s
[+] Wordlist:   subdomains-top1million-5000.txt
===============================================================
Starting gobuster in DNS enumeration mode
===============================================================
Found: smtp.gentoo.org [140.211.166.183]

Found: www.gentoo.org [151.101.1.91,151.101.65.91,151.101.129.91,151.101.193.91]

Found: mail.gentoo.org [140.211.166.183]

Found: ns2.gentoo.org [154.52.129.30]

Found: ns1.gentoo.org [140.211.166.189]

Found: dev.gentoo.org [140.211.166.183]

Found: admin.gentoo.org [140.211.166.162]

Found: ns3.gentoo.org [65.98.29.106]

Found: test.gentoo.org [140.211.166.176]

Found: ns4.gentoo.org [176.119.25.15]

Found: lists.gentoo.org [208.92.234.80]

Found: wiki.gentoo.org [140.211.166.177]

Found: api.gentoo.org [212.102.50.5,212.102.50.11,212.102.50.2,212.102.50.8]

Found: store.gentoo.org [89.238.71.5,89.16.167.139]

Found: forums.gentoo.org [140.211.166.177]

Found: blogs.gentoo.org [140.211.166.176]

Progress: 162 / 4990 (3.25%)
```

5.指定DNS解析超时时间（--timeout）

不设置的情况下默认为1s超时，通过**--timeout**可以指定，比如指定超时时间为0.5s可以是：

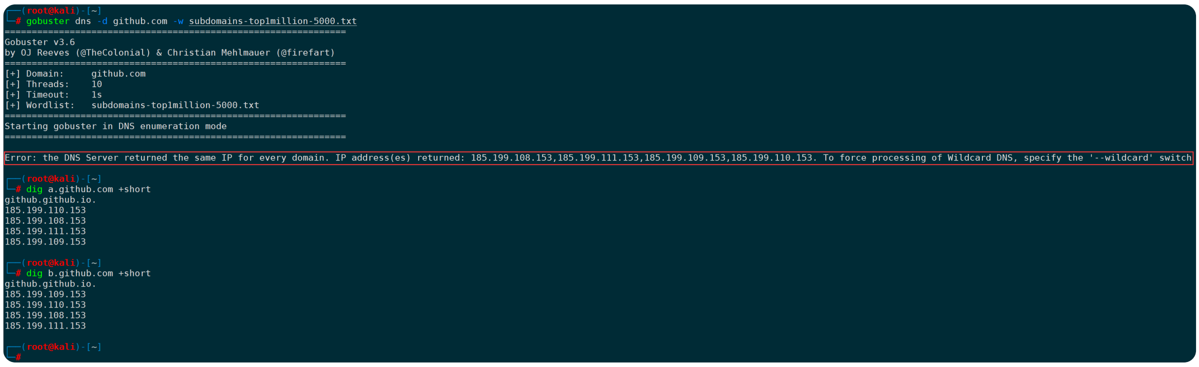
```
gobuster dns -d <domain> -w <wordlist> --timeout 0.5s
```



```
┌──(root@kali)-[~]
└─# gobuster dns -d linux-code.com -w subdomains-top1million-5000.txt --timeout 0.5s
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     linux-code.com
[+] Threads:    10
[+] Timeout:    500ms
[+] Wordlist:   subdomains-top1million-5000.txt
===============================================================
Starting gobuster in DNS enumeration mode
===============================================================
Found: blog.linux-code.com

Found: wap.linux-code.com

Found: files.linux-code.com

Found: docs.linux-code.com

Found: data.linux-code.com

Found: cloud.linux-code.com

Found: music.linux-code.com

Found: vip.linux-code.com

Found: storage.linux-code.com

Found: cc.linux-code.com

Found: terminal.linux-code.com

Found: wifi.linux-code.com

Found: vcenter.linux-code.com
```

6.通配符域名的强制处理（--wildcard)

如果目标域名的子域名为通配符域名，形如 ***.domain.com**，那么字典里面的子域名记录，不管是什么都能返回解析记录，比如github官网：

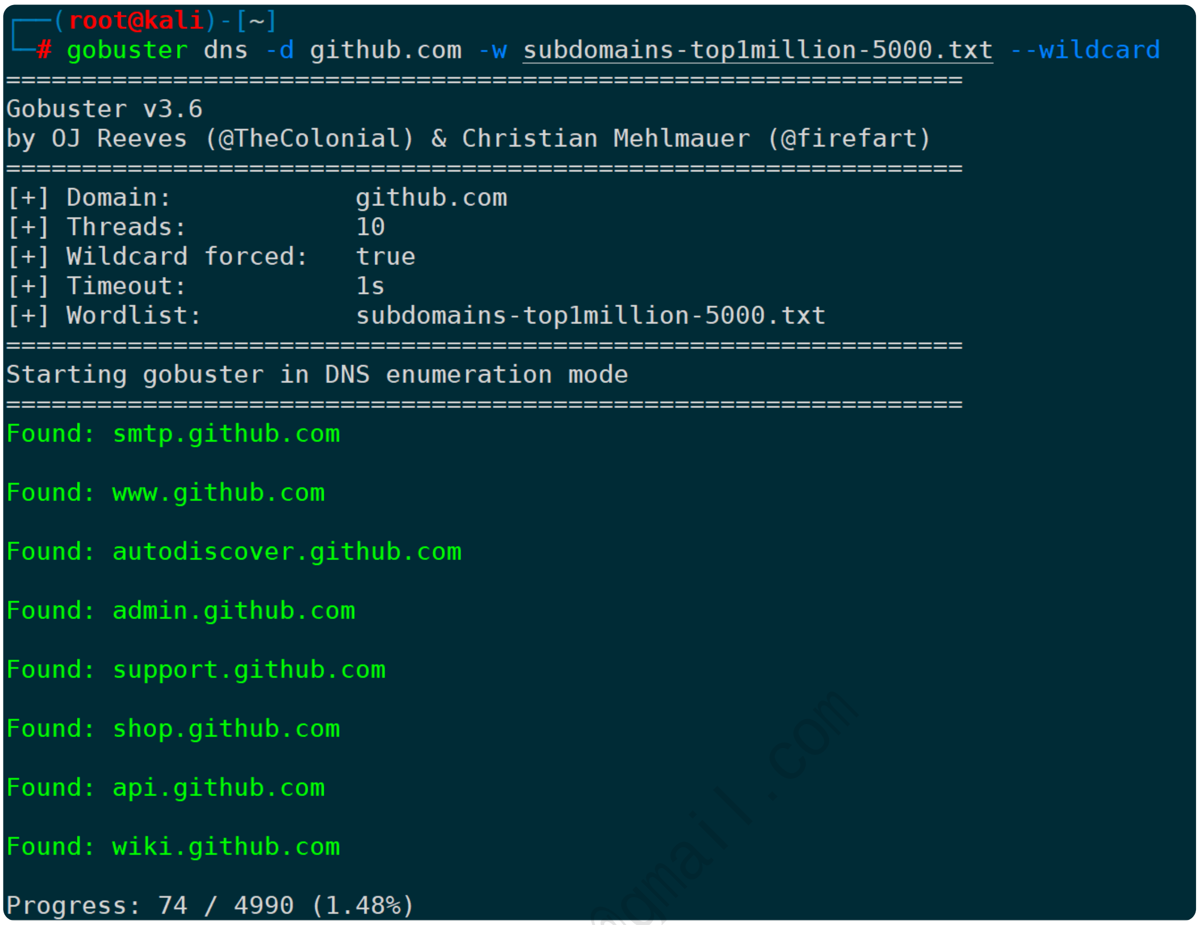


```
┌──(root@kali)-[~]
└─# gobuster dns -d github.com -w subdomains-top1million-5000.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     github.com
[+] Threads:    10
[+] Timeout:    1s
[+] Wordlist:   subdomains-top1million-5000.txt
===============================================================
Starting gobuster in DNS enumeration mode
===============================================================

Error: the DNS Server returned the same IP for every domain. IP address(es) returned: 185.199.108.153,185.199.111.153,185.199.109.153,185.199.110.153. To force processing of Wildcard DNS, specify the '--wildcard' switch

┌──(root@kali)-[~]
└─# dig a.github.com +short
github.github.io.
185.199.110.153
185.199.108.153
185.199.111.153
185.199.109.153

┌──(root@kali)-[~]
└─# dig b.github.com +short
github.github.io.
185.199.109.153
185.199.110.153
185.199.108.153
185.199.111.153

┌──(root@kali)-[~]
└─#
```

如上图，gobuster执行后会提示几乎每个域名都返回同样的A记录结果，通过dig也能测试出来。

此时我们指定**--wildcard**参数，wildcard直译为通配符，让gobuster遇到通配符域名时继续强制执行，但只会返回和通配符域名不一样的解析结果的域名（这个逻辑判断是正确的，不然字典里每个字段都能解析出地址没有任何意义）：

```
gobuster dns -d <domain> -w <wordlist> --wildcard
```

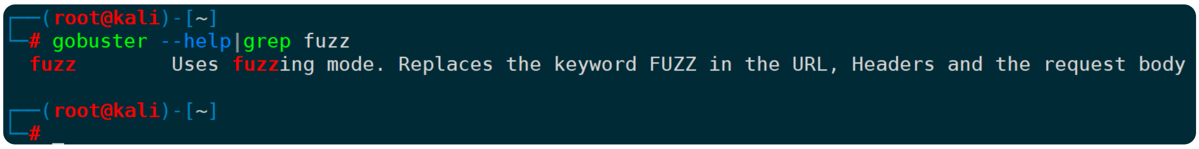


```
┌─(root@kali)-[~]
└─# gobuster dns -d github.com -w subdomains-top1million-5000.txt --wildcard
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:            github.com
[+] Threads:           10
[+] Wildcard forced:   true
[+] Timeout:           1s
[+] Wordlist:          subdomains-top1million-5000.txt
===============================================================
Starting gobuster in DNS enumeration mode
===============================================================
Found: smtp.github.com

Found: www.github.com

Found: autodiscover.github.com

Found: admin.github.com

Found: support.github.com

Found: shop.github.com

Found: api.github.com

Found: wiki.github.com

Progress: 74 / 4990 (1.48%)
```

六、模糊模式暴力枚举（fuzz）

Uses fuzzing mode. Replaces the keyword FUZZ in the URL, Headers and the request body.

正如帮助文档所述，fuzz模式可以替换FUZZ关键字在URL或者HTTP头部以及请求体里面：



```
┌─(root@kali)-[~]
└─# gobuster --help|grep fuzz
  fuzz        Uses fuzzing mode. Replaces the keyword FUZZ in the URL, Headers and the request body

┌─(root@kali)-[~]
└─# _
```

这么说可能比较抽象，可以理解构造的请求URL、HTTP头部、发送的请求体只要掺杂fuzz，就可以带入fuzz变量，fuzz变量的值来源于字典内容，一个个替换到fuzz变量上进行枚举。

比如URL参数枚举，可以写成：

```
http://example.com/profile?user=FUZZ
```

再比如HTTP头部内的某个字段枚举，比如枚举UA信息：

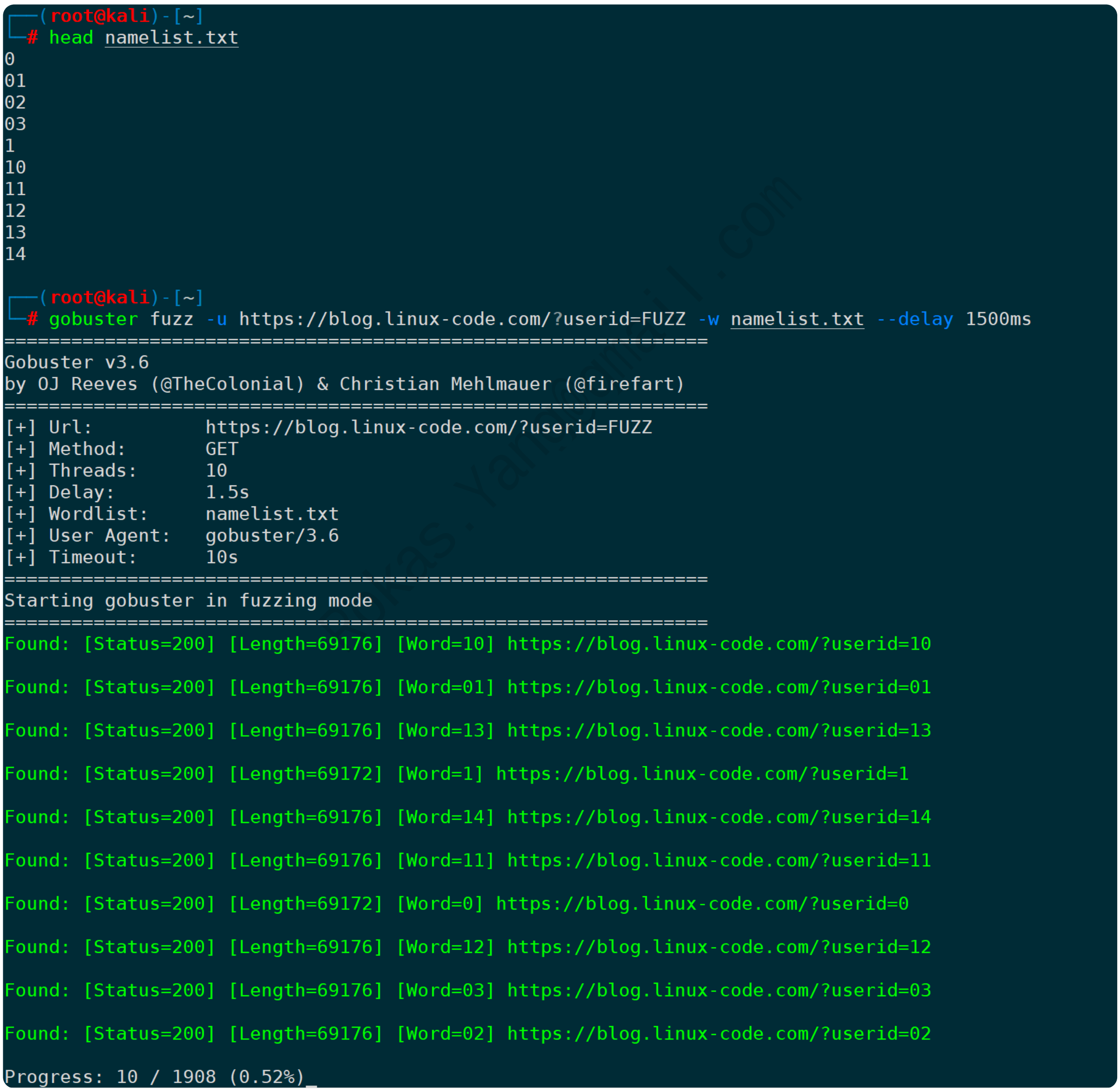
```
-H 'User-Agent: FUZZ'
```

除了以上功能，其他参数都和dir模式完全一致，下面只举例两种最常见的情况，其他任何复杂场景都可以按需配合FUZZ构造请求。

1.指定URL并枚举用户名（-u）

比如枚举一个固定URL，通过入参字典里的字段内容，来进行穷举：

```
gobuster fuzz -u domain/?userid=FUZZ -w <wordlist>
```



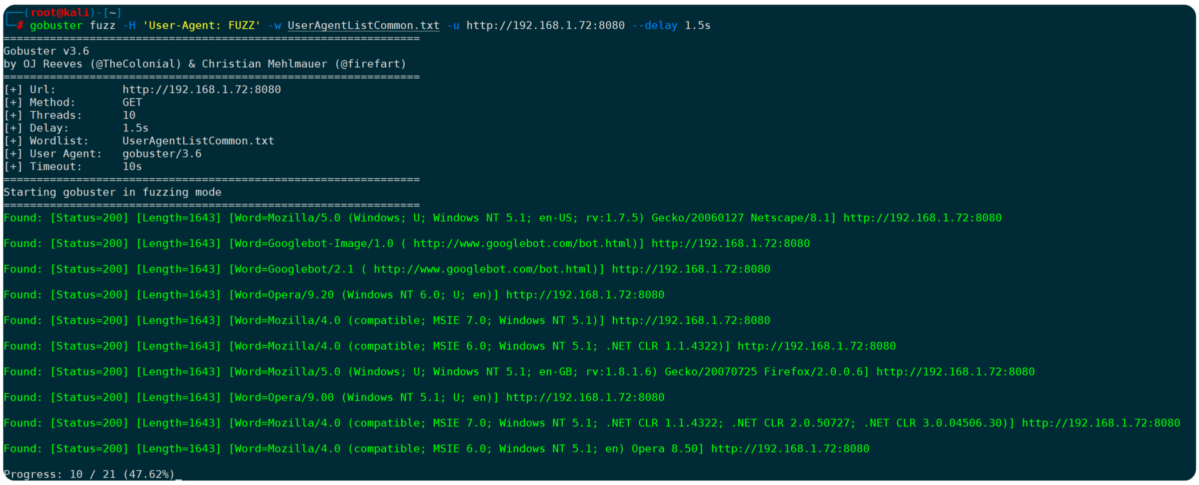
```
┌──(root㉿kali)-[~]
└─# head namelist.txt
0
01
02
03
1
10
11
12
13
14

┌──(root㉿kali)-[~]
└─# gobuster fuzz -u https://blog.linux-code.com/?userid=FUZZ -w namelist.txt --delay 1500ms
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:            https://blog.linux-code.com/?userid=FUZZ
[+] Method:         GET
[+] Threads:        10
[+] Delay:          1.5s
[+] Wordlist:       namelist.txt
[+] User Agent:     gobuster/3.6
[+] Timeout:        10s
===============================================================
Starting gobuster in fuzzing mode
===============================================================
Found: [Status=200] [Length=69176] [Word=10] https://blog.linux-code.com/?userid=10

Found: [Status=200] [Length=69176] [Word=01] https://blog.linux-code.com/?userid=01

Found: [Status=200] [Length=69176] [Word=13] https://blog.linux-code.com/?userid=13

Found: [Status=200] [Length=69172] [Word=1] https://blog.linux-code.com/?userid=1

Found: [Status=200] [Length=69176] [Word=14] https://blog.linux-code.com/?userid=14

Found: [Status=200] [Length=69176] [Word=11] https://blog.linux-code.com/?userid=11

Found: [Status=200] [Length=69172] [Word=0] https://blog.linux-code.com/?userid=0

Found: [Status=200] [Length=69176] [Word=12] https://blog.linux-code.com/?userid=12

Found: [Status=200] [Length=69176] [Word=03] https://blog.linux-code.com/?userid=03

Found: [Status=200] [Length=69176] [Word=02] https://blog.linux-code.com/?userid=02

Progress: 10 / 1908 (0.52%)_
```

gobuster将字典文件内容逐个替换到FUZZ占位符中进行请求。

2.枚举UA信息（-H）

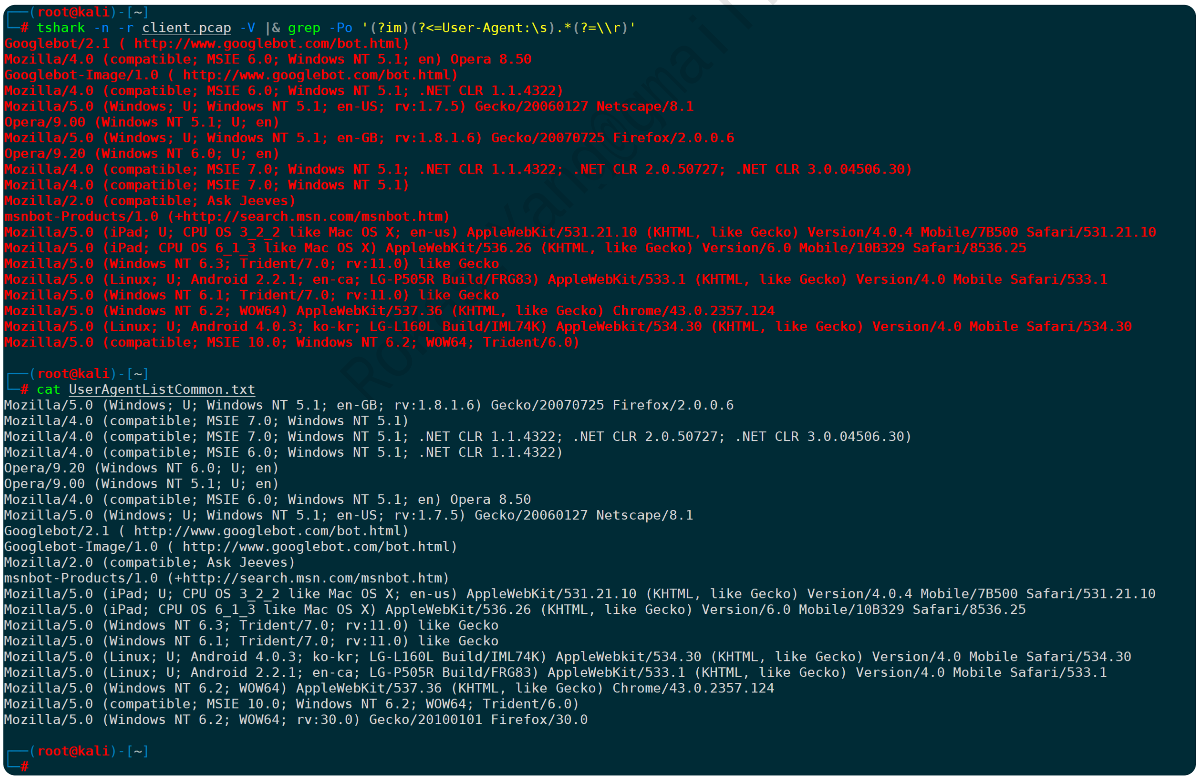
通过UA字典文件的信息，替换到FUZZ占位符：

```
gobuster fuzz -H 'User-Agent: FUZZ' -w <wordlist> -u http://192.168.1.72:8080
```

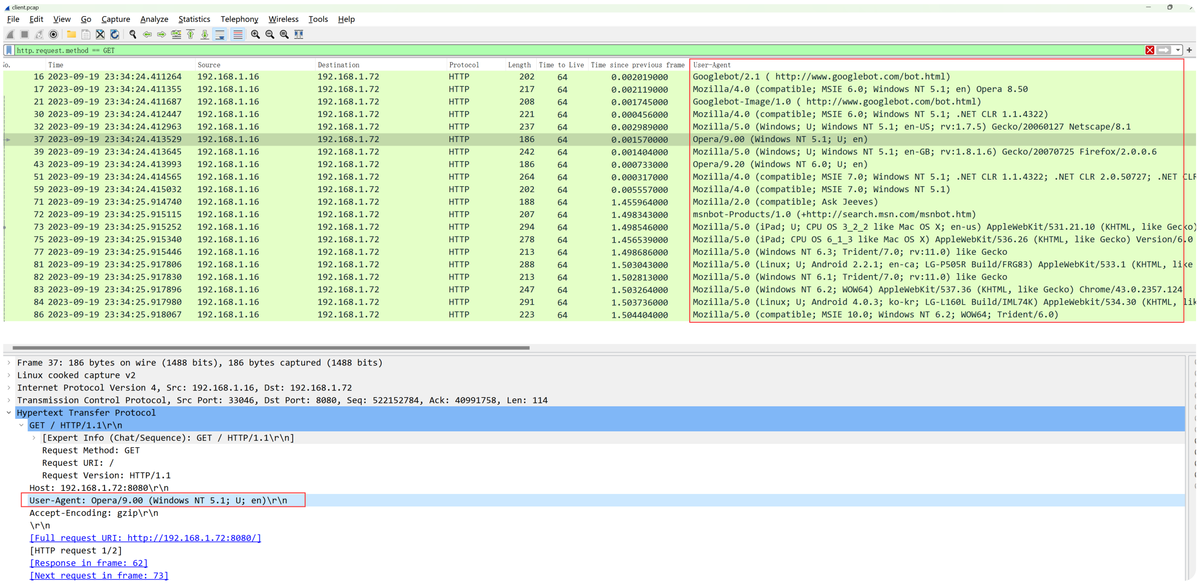


```
┌──(root㉿kali)-[~]
└─# gobuster fuzz -H 'User-Agent: FUZZ' -w UserAgentListCommon.txt -u http://192.168.1.72:8080 --delay 1.5s
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://192.168.1.72:8080
[+] Method:          GET
[+] Threads:         10
[+] Delay:           1.5s
[+] Wordlist:        UserAgentListCommon.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
===============================================================
Starting gobuster in fuzzing mode
===============================================================
Found: [Status=200] [Length=1643] [Word=Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.5) Gecko/20060127 Netscape/8.1] http://192.168.1.72:8080

Found: [Status=200] [Length=1643] [Word=Googlebot-Image/1.0 ( http://www.googlebot.com/bot.html)] http://192.168.1.72:8080

Found: [Status=200] [Length=1643] [Word=Googlebot/2.1 ( http://www.googlebot.com/bot.html)] http://192.168.1.72:8080

Found: [Status=200] [Length=1643] [Word=Opera/9.20 (Windows NT 6.0; U; en)] http://192.168.1.72:8080

Found: [Status=200] [Length=1643] [Word=Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)] http://192.168.1.72:8080

Found: [Status=200] [Length=1643] [Word=Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)] http://192.168.1.72:8080

Found: [Status=200] [Length=1643] [Word=Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6] http://192.168.1.72:8080

Found: [Status=200] [Length=1643] [Word=Opera/9.00 (Windows NT 5.1; U; en)] http://192.168.1.72:8080

Found: [Status=200] [Length=1643] [Word=Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)] http://192.168.1.72:8080

Found: [Status=200] [Length=1643] [Word=Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; en) Opera 8.50] http://192.168.1.72:8080

Progress: 10 / 21 (47.62%)_
```

通过抓包也可以发现，HTTP头部里的UA信息将从字典文件里逐个代入：



```
┌──(root㉿kali)-[~]
└─# tshark -n -r client.pcap -V |& grep -Po '(?im)(?<=User-Agent:\s).*(?=\\r)'
Googlebot/2.1 ( http://www.googlebot.com/bot.html)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; en) Opera 8.50
Googlebot-Image/1.0 ( http://www.googlebot.com/bot.html)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.5) Gecko/20060127 Netscape/8.1
Opera/9.00 (Windows NT 5.1; U; en)
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6
Opera/9.20 (Windows NT 6.0; U; en)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
Mozilla/2.0 (compatible; Ask Jeeves)
msnbot-Products/1.0 (+http://search.msn.com/msnbot.htm)
Mozilla/5.0 (iPad; U; CPU OS 3_2_2 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like Gecko) Version/4.0.4 Mobile/7B500 Safari/531.21.10
Mozilla/5.0 (iPad; CPU OS 6_1_3 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10B329 Safari/8536.25
Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
Mozilla/5.0 (Linux; U; Android 2.2.1; en-ca; LG-P505R Build/FRG83) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1
Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.124
Mozilla/5.0 (Linux; U; Android 4.0.3; ko-kr; LG-L160L Build/IML74K) AppleWebkit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)

┌──(root㉿kali)-[~]
└─# cat UserAgentListCommon.txt
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
Opera/9.20 (Windows NT 6.0; U; en)
Opera/9.00 (Windows NT 5.1; U; en)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; en) Opera 8.50
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.5) Gecko/20060127 Netscape/8.1
Googlebot/2.1 ( http://www.googlebot.com/bot.html)
Googlebot-Image/1.0 ( http://www.googlebot.com/bot.html)
Mozilla/2.0 (compatible; Ask Jeeves)
msnbot-Products/1.0 (+http://search.msn.com/msnbot.htm)
Mozilla/5.0 (iPad; U; CPU OS 3_2_2 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like Gecko) Version/4.0.4 Mobile/7B500 Safari/531.21.10
Mozilla/5.0 (iPad; CPU OS 6_1_3 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10B329 Safari/8536.25
Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Mozilla/5.0 (Linux; U; Android 4.0.3; ko-kr; LG-L160L Build/IML74K) AppleWebkit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30
Mozilla/5.0 (Linux; U; Android 2.2.1; en-ca; LG-P505R Build/FRG83) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1
Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.124
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)
Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0

┌──(root㉿kali)-[~]
└─#
```



http.request.method == GET

```
o.    Time                        Source          Destination     Protocol  Length  Time to Live  Time since previous frame  User-Agent
   16 2023-09-19 23:34:24.411264  192.168.1.16    192.168.1.72    HTTP      202     64            0.002019000                Googlebot/2.1 ( http://www.googlebot.com/bot.html)
   17 2023-09-19 23:34:24.411355  192.168.1.16    192.168.1.72    HTTP      217     64            0.002119000                Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; en) Opera 8.50
   21 2023-09-19 23:34:24.411687  192.168.1.16    192.168.1.72    HTTP      208     64            0.001745000                Googlebot-Image/1.0 ( http://www.googlebot.com/bot.html)
   30 2023-09-19 23:34:24.412447  192.168.1.16    192.168.1.72    HTTP      221     64            0.000456000                Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
   32 2023-09-19 23:34:24.412963  192.168.1.16    192.168.1.72    HTTP      237     64            0.002989000                Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.5) Gecko/20060127 Netscape/8.1
   37 2023-09-19 23:34:24.413529  192.168.1.16    192.168.1.72    HTTP      186     64            0.001570000                Opera/9.00 (Windows NT 5.1; U; en)
   39 2023-09-19 23:34:24.413645  192.168.1.16    192.168.1.72    HTTP      242     64            0.001404000                Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6
   43 2023-09-19 23:34:24.413993  192.168.1.16    192.168.1.72    HTTP      186     64            0.000733000                Opera/9.20 (Windows NT 6.0; U; en)
   51 2023-09-19 23:34:24.414565  192.168.1.16    192.168.1.72    HTTP      264     64            0.000317000                Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR
   59 2023-09-19 23:34:24.415032  192.168.1.16    192.168.1.72    HTTP      202     64            0.005557000                Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
   71 2023-09-19 23:34:25.914740  192.168.1.16    192.168.1.72    HTTP      188     64            1.455964000                Mozilla/2.0 (compatible; Ask Jeeves)
   72 2023-09-19 23:34:25.915115  192.168.1.16    192.168.1.72    HTTP      207     64            1.498343000                msnbot-Products/1.0 (+http://search.msn.com/msnbot.htm)
   73 2023-09-19 23:34:25.915252  192.168.1.16    192.168.1.72    HTTP      294     64            1.498546000                Mozilla/5.0 (iPad; U; CPU OS 3_2_2 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like Gecko)
   75 2023-09-19 23:34:25.915340  192.168.1.16    192.168.1.72    HTTP      278     64            1.456539000                Mozilla/5.0 (iPad; CPU OS 6_1_3 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0
   77 2023-09-19 23:34:25.915446  192.168.1.16    192.168.1.72    HTTP      213     64            1.498686000                Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
   81 2023-09-19 23:34:25.917806  192.168.1.16    192.168.1.72    HTTP      288     64            1.503043000                Mozilla/5.0 (Linux; U; Android 2.2.1; en-ca; LG-P505R Build/FRG83) AppleWebKit/533.1 (KHTML, like
   82 2023-09-19 23:34:25.917830  192.168.1.16    192.168.1.72    HTTP      213     64            1.502813000                Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
   83 2023-09-19 23:34:25.917896  192.168.1.16    192.168.1.72    HTTP      247     64            1.503264000                Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.124
   84 2023-09-19 23:34:25.917980  192.168.1.16    192.168.1.72    HTTP      291     64            1.503736000                Mozilla/5.0 (Linux; U; Android 4.0.3; ko-kr; LG-L160L Build/IML74K) AppleWebkit/534.30 (KHTML, lik
   86 2023-09-19 23:34:25.918067  192.168.1.16    192.168.1.72    HTTP      223     64            1.504404000                Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)
```

```
> Frame 37: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits)
> Linux cooked capture v2
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.72
> Transmission Control Protocol, Src Port: 33046, Dst Port: 8080, Seq: 522152784, Ack: 40991758, Len: 114
v Hypertext Transfer Protocol
  v GET / HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Host: 192.168.1.72:8080\r\n
    User-Agent: Opera/9.00 (Windows NT 5.1; U; en)\r\n
    Accept-Encoding: gzip\r\n
    \r\n
    [Full request URI: http://192.168.1.72:8080/]
    [HTTP request 1/2]
    [Response in frame: 62]
    [Next request in frame: 73]
```

七、基于虚拟主机的暴力枚举（vhost）

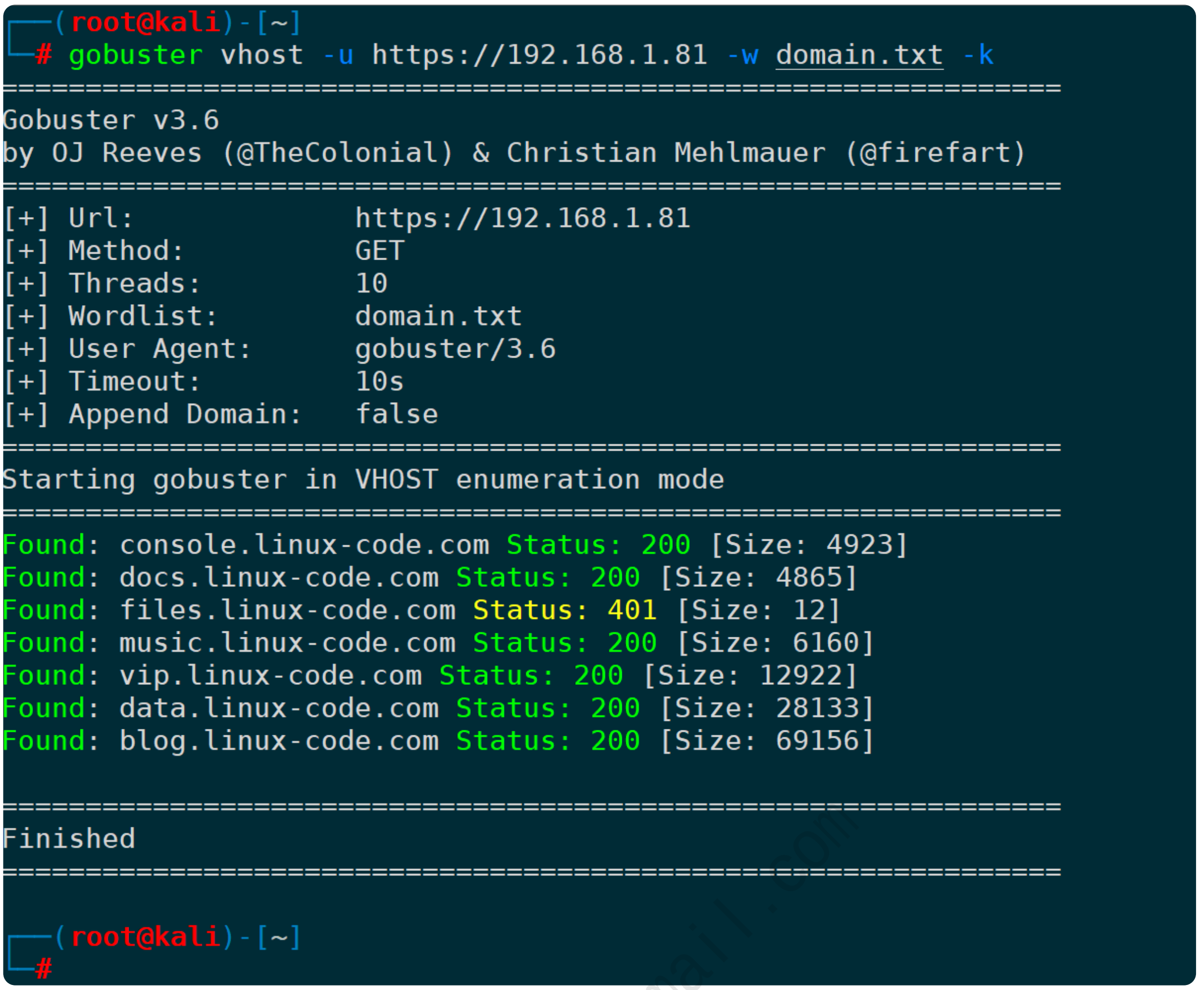
想知道一个目的IP有哪些对应的服务域名/虚拟主机时，**vhost**则非常有用，特别是通过DNS模式拿到子域名列表后，可以尝试通过不同的解析IP去枚举上面是否存在这些子域名服务。

其中大部分参数和**dir模式**是通用的，使用方法也一样，因此不反复赘述，下面将列举较为经典的几个场景。

1.指定URL进行虚拟主机枚举（-u）

URL写成IP形式，主机名存放在字典里，**-k**不进行TLS/SSL证书校验：

```
gobuster vhost -u <URL> -w <wordlist> -k
```



```
┌──(root@kali)-[~]
└─# gobuster vhost -u https://192.168.1.81 -w domain.txt -k
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             https://192.168.1.81
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        domain.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   false
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: console.linux-code.com Status: 200 [Size: 4923]
Found: docs.linux-code.com Status: 200 [Size: 4865]
Found: files.linux-code.com Status: 401 [Size: 12]
Found: music.linux-code.com Status: 200 [Size: 6160]
Found: vip.linux-code.com Status: 200 [Size: 12922]
Found: data.linux-code.com Status: 200 [Size: 28133]
Found: blog.linux-code.com Status: 200 [Size: 69156]

===============================================================
Finished
===============================================================

┌──(root@kali)-[~]
└─#
```

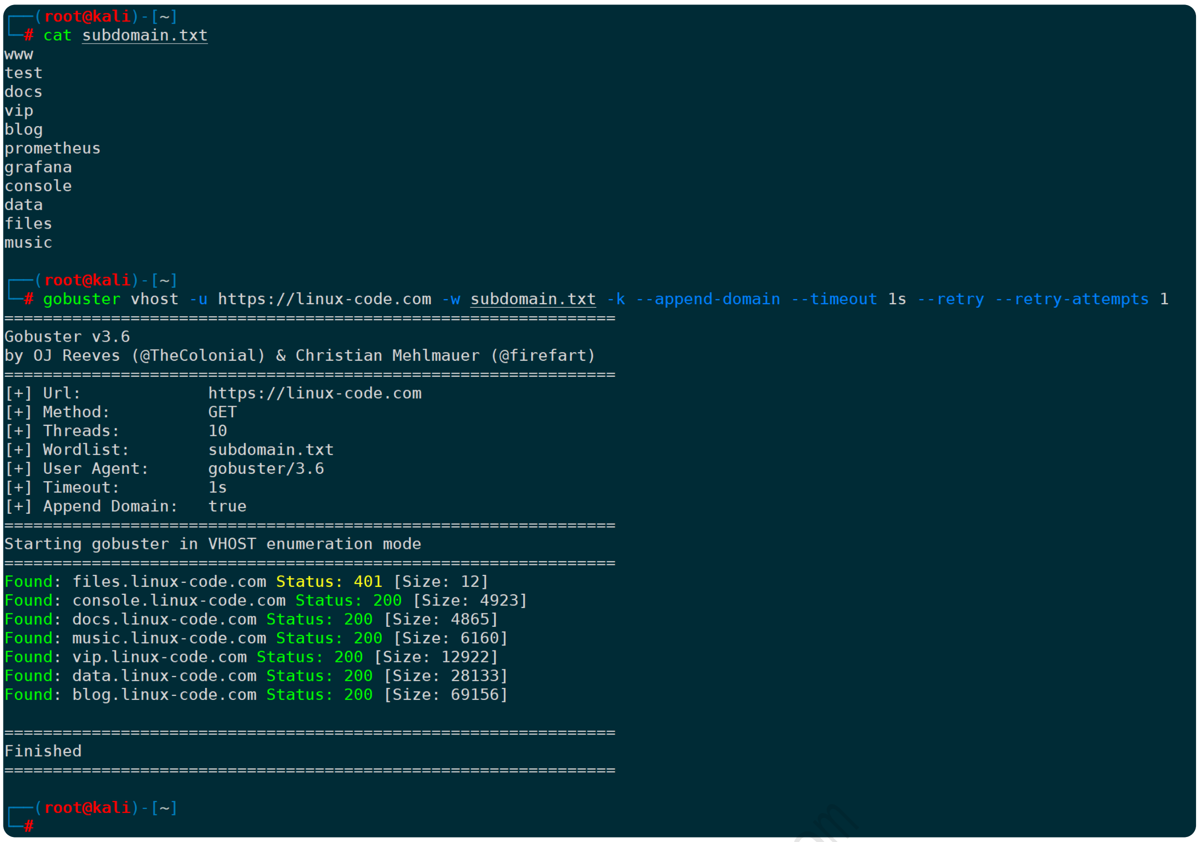
2.附加主机名子域（--append-domain）

此参数会将字典里的内容，添加到URL的HOST之前，比如URL为： https://domain.com ， 读取字典内容（如a、b、c），填充后的HOST为：**a.domain.com**、**b.domain.com**、 **c.domain.com**。

> 如果URL是IP或者IP:PORT形式，那么照样会在前面加，比如： `a.192.168.1.72:8080`、`a.192.168.1.1`。

举个例子，指定的URL已经是主域名形式，指定子域名字典subdomain.txt进行虚拟主机的枚举可以是：

```
gobuster vhost -u <URL> -w subdomain.txt -k --append-domain --timeout 1s --retry --retry-attempts 1
```



```
┌──(root㉿kali)-[~]
└─# cat subdomain.txt
www
test
docs
vip
blog
prometheus
grafana
console
data
files
music

┌──(root㉿kali)-[~]
└─# gobuster vhost -u https://linux-code.com -w subdomain.txt -k --append-domain --timeout 1s --retry --retry-attempts 1
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             https://linux-code.com
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        subdomain.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         1s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: files.linux-code.com Status: 401 [Size: 12]
Found: console.linux-code.com Status: 200 [Size: 4923]
Found: docs.linux-code.com Status: 200 [Size: 4865]
Found: music.linux-code.com Status: 200 [Size: 6160]
Found: vip.linux-code.com Status: 200 [Size: 12922]
Found: data.linux-code.com Status: 200 [Size: 28133]
Found: blog.linux-code.com Status: 200 [Size: 69156]

===============================================================
Finished
===============================================================

┌──(root㉿kali)-[~]
└─#
```

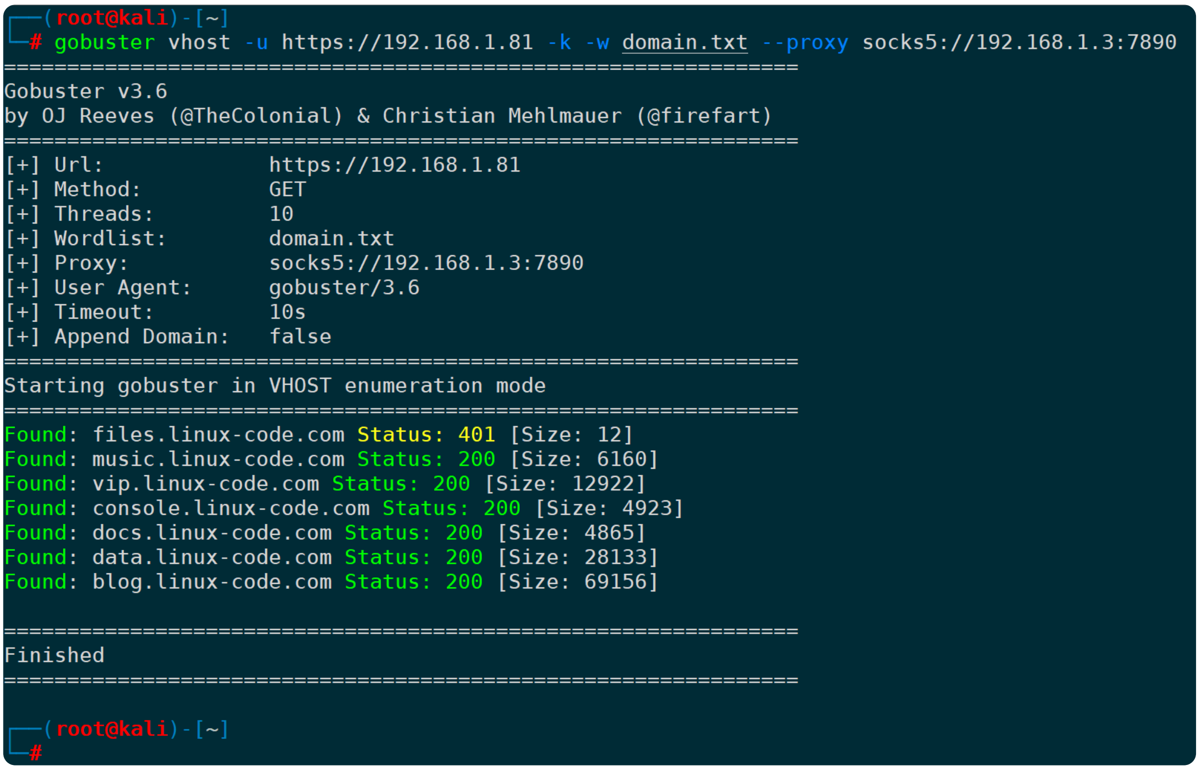
- **--timeout 1s**：设置超时时间为1s，不指定默认10s。
- **--retry**：超时后重试。
- **--retry-attempts 1**：设置最大重试次数1次，不指定默认3次。

这里需要和DNS子域枚举区分开来，它并涉及DNS解析请求，**vhost**模式会对组合出来的所有HOST都默认发送HTTP GET请求，其它HTTP方法，通过**-m**参数指定即可，比如**-m POST**。

3.指定代理服务器（--proxy）

因为需要向对端发送HTTP/HTTPS请求，并不想暴露自己的情况下，可以使用代理，和**dir模式**一样，支持HTTP/HTTPS/socks5代理，以socks5代理为例：

```
gobuster vhost -u <URL> -k -w <wordlist> --proxy <socks5://host:port>
```

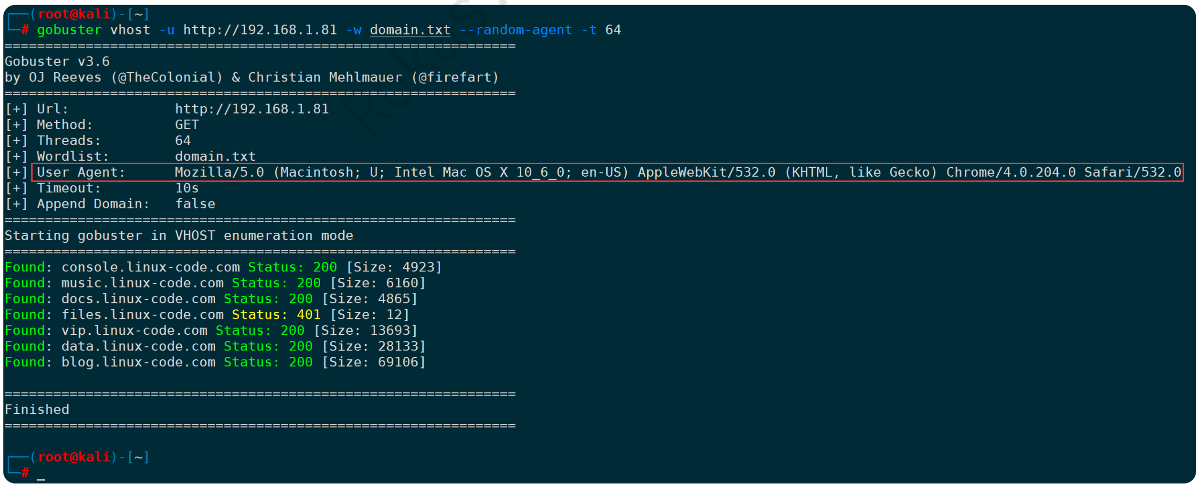


```
┌──(root@kali)-[~]
└─# gobuster vhost -u https://192.168.1.81 -k -w domain.txt --proxy socks5://192.168.1.3:7890
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://192.168.1.81
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                domain.txt
[+] Proxy:                   socks5://192.168.1.3:7890
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
[+] Append Domain:           false
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: files.linux-code.com Status: 401 [Size: 12]
Found: music.linux-code.com Status: 200 [Size: 6160]
Found: vip.linux-code.com Status: 200 [Size: 12922]
Found: console.linux-code.com Status: 200 [Size: 4923]
Found: docs.linux-code.com Status: 200 [Size: 4865]
Found: data.linux-code.com Status: 200 [Size: 28133]
Found: blog.linux-code.com Status: 200 [Size: 69156]

===============================================================
Finished
===============================================================

┌──(root@kali)-[~]
└─#
```

4.随机User-Agent（--random-agent）

伪造UA信息，提升真实信息的隐蔽性，给对方访问日志也造成一种干扰：

```
gobuster vhost -u <URL> -w <wordlist> --random-agent -t 64  # -t指定线程数量
```



```
┌──(root@kali)-[~]
└─# gobuster vhost -u http://192.168.1.81 -w domain.txt --random-agent -t 64
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.81
[+] Method:                  GET
[+] Threads:                 64
[+] Wordlist:                domain.txt
[+] User Agent:              Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_0; en-US) AppleWebKit/532.0 (KHTML, like Gecko) Chrome/4.0.204.0 Safari/532.0
[+] Timeout:                 10s
[+] Append Domain:           false
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: console.linux-code.com Status: 200 [Size: 4923]
Found: music.linux-code.com Status: 200 [Size: 6160]
Found: docs.linux-code.com Status: 200 [Size: 4865]
Found: files.linux-code.com Status: 401 [Size: 12]
Found: vip.linux-code.com Status: 200 [Size: 13693]
Found: data.linux-code.com Status: 200 [Size: 28133]
Found: blog.linux-code.com Status: 200 [Size: 69106]

===============================================================
Finished
===============================================================

┌──(root@kali)-[~]
└─# _
```

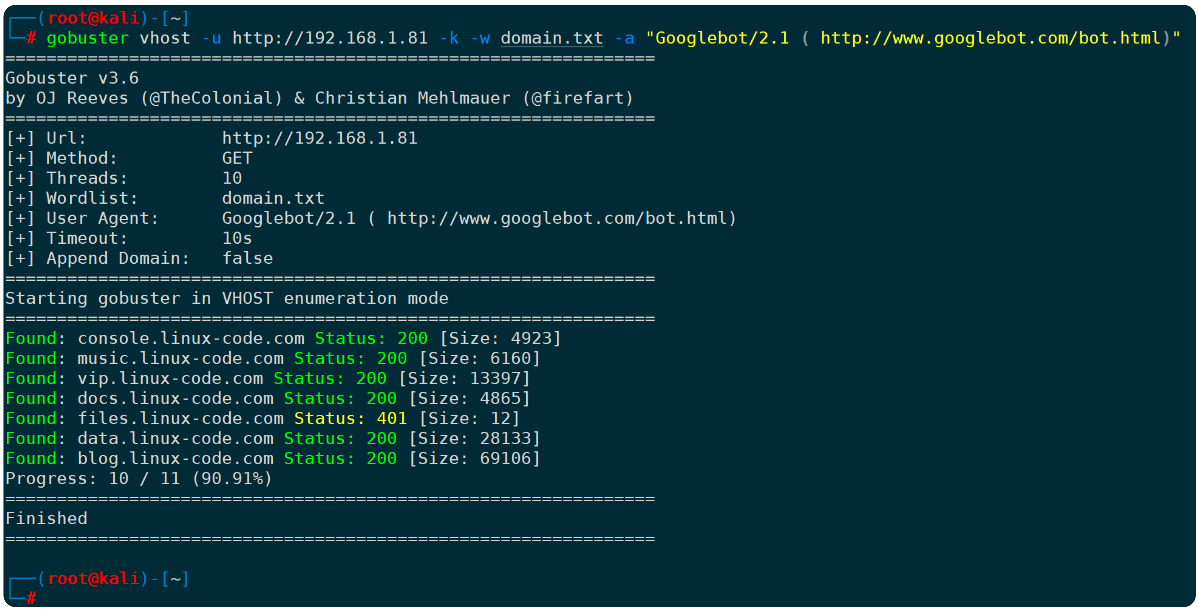
如上图，构造了一个MacOS客户端且浏览器为Chrome的虚假UA信息。

5.指定User-Agent（-a|--useragent）

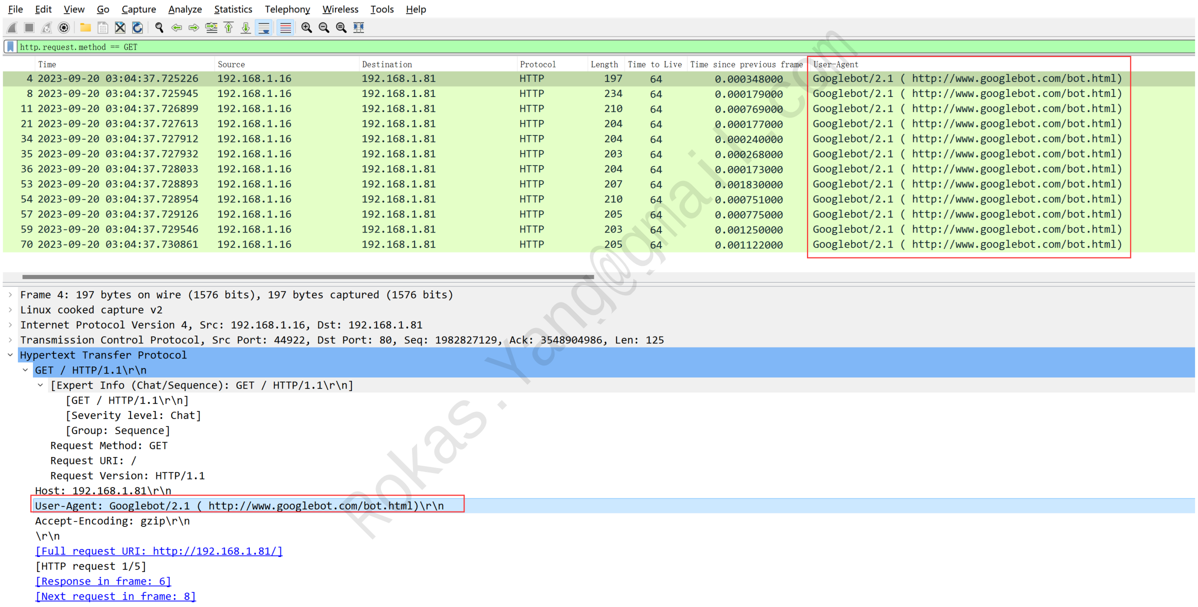
实际上也可以通过-H参数来从HTTP头部参数里指定，参照**dir模式**的-H。

通过此参数来指定，可以伪造我们想伪造的任何UA信息，比如伪造为谷歌bot可以是：

```
gobuster vhost -u <URL> -w <wordlist> -a "Googlebot/2.1 ( 
http://www.googlebot.com/bot.html)"
```



```
┌──(root㉿kali)-[~]
└─# gobuster vhost -u http://192.168.1.81 -k -w domain.txt -a "Googlebot/2.1 ( http://www.googlebot.com/bot.html)"
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://192.168.1.81
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        domain.txt
[+] User Agent:      Googlebot/2.1 ( http://www.googlebot.com/bot.html)
[+] Timeout:         10s
[+] Append Domain:   false
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: console.linux-code.com Status: 200 [Size: 4923]
Found: music.linux-code.com Status: 200 [Size: 6160]
Found: vip.linux-code.com Status: 200 [Size: 13397]
Found: docs.linux-code.com Status: 200 [Size: 4865]
Found: files.linux-code.com Status: 401 [Size: 12]
Found: data.linux-code.com Status: 200 [Size: 28133]
Found: blog.linux-code.com Status: 200 [Size: 69106]
Progress: 10 / 11 (90.91%)
===============================================================
Finished
===============================================================

┌──(root㉿kali)-[~]
└─#
```



http.request.method == GET

	Time	Source	Destination	Protocol	Length	Time to Live	Time since previous frame	User-Agent
4	2023-09-20 03:04:37.725226	192.168.1.16	192.168.1.81	HTTP	197	64	0.000348000	Googlebot/2.1 (http://www.googlebot.com/bot.html)
8	2023-09-20 03:04:37.725945	192.168.1.16	192.168.1.81	HTTP	234	64	0.000179000	Googlebot/2.1 (http://www.googlebot.com/bot.html)
11	2023-09-20 03:04:37.726899	192.168.1.16	192.168.1.81	HTTP	210	64	0.000769000	Googlebot/2.1 (http://www.googlebot.com/bot.html)
21	2023-09-20 03:04:37.727613	192.168.1.16	192.168.1.81	HTTP	204	64	0.000177000	Googlebot/2.1 (http://www.googlebot.com/bot.html)
34	2023-09-20 03:04:37.727912	192.168.1.16	192.168.1.81	HTTP	204	64	0.000240000	Googlebot/2.1 (http://www.googlebot.com/bot.html)
35	2023-09-20 03:04:37.727932	192.168.1.16	192.168.1.81	HTTP	203	64	0.000268000	Googlebot/2.1 (http://www.googlebot.com/bot.html)
36	2023-09-20 03:04:37.728033	192.168.1.16	192.168.1.81	HTTP	204	64	0.000173000	Googlebot/2.1 (http://www.googlebot.com/bot.html)
53	2023-09-20 03:04:37.728893	192.168.1.16	192.168.1.81	HTTP	207	64	0.001830000	Googlebot/2.1 (http://www.googlebot.com/bot.html)
54	2023-09-20 03:04:37.728954	192.168.1.16	192.168.1.81	HTTP	210	64	0.000751000	Googlebot/2.1 (http://www.googlebot.com/bot.html)
57	2023-09-20 03:04:37.729126	192.168.1.16	192.168.1.81	HTTP	205	64	0.000775000	Googlebot/2.1 (http://www.googlebot.com/bot.html)
59	2023-09-20 03:04:37.729546	192.168.1.16	192.168.1.81	HTTP	203	64	0.001250000	Googlebot/2.1 (http://www.googlebot.com/bot.html)
70	2023-09-20 03:04:37.730861	192.168.1.16	192.168.1.81	HTTP	205	64	0.001122000	Googlebot/2.1 (http://www.googlebot.com/bot.html)

```
› Frame 4: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits)
› Linux cooked capture v2
› Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.81
› Transmission Control Protocol, Src Port: 44922, Dst Port: 80, Seq: 1982827129, Ack: 3548904986, Len: 125
⌄ Hypertext Transfer Protocol
  ⌄ GET / HTTP/1.1\r\n
    ⌄ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
        [GET / HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Host: 192.168.1.81\r\n
    User-Agent: Googlebot/2.1 ( http://www.googlebot.com/bot.html)\r\n
    Accept-Encoding: gzip\r\n
    \r\n
    [Full request URI: http://192.168.1.81/]
    [HTTP request 1/5]
    [Response in frame: 6]
    [Next request in frame: 8]
```

八、总结

Gobuster作为web安全、渗透领域的案头常备利器之一，其功能全面且强大，支持多线程高并发请求，常用于发现Web应用程序中隐藏的目录和文件，以及对子域名、虚拟主机vhost等进行暴力枚举等场景。

同时也通过抓包分析了不同场景的参数选择上的差异和行为。选择合适的字典文件可以显著影响扫描的效率和成功率，本文也整理了业内极具知名度并且覆盖各类场景的字典，可以作为参考按照实际情况去二次生成更适配需求的字典。

总的来说，Gobuster是渗透测试工具箱中不可或缺的一部分，它可以帮助渗透测试人员识别Web应用程序中的潜在漏洞和安全风险。