

hashcat使用

Hashcat 是一款用于破解密码的工具，据说是世界上最快最高级的密码破解工具，支持 LM 哈希、MD5、SHA 等系列的密码破解，同时也支持 Linux、Mac、Windows 平台。

参数：

```
-r 使用自定义破解规则
-o 指定破解成功后的 hash 及所对应的明文密码的存放位置
-m 指定要破解的 hash 类型，如果不指定类型，则默认是 MD5
-a 指定要使用的破解模式，其值参考后面对参数。“-a 0”字典攻击，“-a 1”组合攻击；“-a 3”掩码攻击
-D 指定 opengl 的设备类型
--show 显示已经破解的 hash 及该 hash 所对应的明文
--force 忽略破解过程中的警告信息，跑单条 hash 可能需要加上此选项
--remove 删除已被破解成功的 hash
--username 忽略 hash 文件中的指定的用户名，在破解 linux 系统用户密码 hash 可能会用到
--increment 启用增量破解模式，你可以利用此模式让 hashcat 在指定的密码长度范围内执行破解过程
--increment-min 密码最小长度，后面直接等于一个整数即可，配置 increment 模式一起使用
--increment-max 密码最大长度，同上
--outfile-format 指定破解结果的输出格式 id，默认是 3
--self-test-disable 关闭启动自检
```

-a 破解模式：

```
0 | Straight          （字段破解）
1 | Combination      （组合破解）
3 | Brute-force      （掩码暴力破解）
6 | Hybrid wordlist + Mask （字典+掩码破解）
7 | Hybrid Mask + wordlist （掩码+字典破解）
```

一般使用 -D 2 指定 GPU 破解

掩码设置：

l	abcdefghijklmnopqrstuvwxyz	纯小写字母
u	ABCDEFGHIJKLMNOPQRSTUVWXYZ	纯大写字母
d	0123456789	纯数字
h	0123456789abcdef	十六进制小写字母和数字
H	0123456789ABCDEF	十六进制大写字母和数字
s	!"#\$%&'()*+,-./:;<=>?@[\\]^_`{ }~	特殊字符
a	?l?u?d?s	键盘上所有可见的字符
b	0x00 - 0xff	匹配密码空格

掩码设置举例：

八位数字密码: ?d?d?d?d?d?d?d?d
八位未知密码: ?a?a?a?a?a?a?a
前四位为大写字母, 后面四位为数字: ?u?u?u?u?d?d?d?d
前四位为数字或者是小写字母, 后四位为大写字母或者数字: ?h?h?h?h?H?H?H?H
前三个字符未知, 中间为admin, 后三位未知: ?a?a?aadmin?a?a?a
6-8位数字密码: --increment --increment-min 6 --increment-max 8 ?d?d?d?d?d?d?d?d
6-8位数字+小写字母密码: --increment --increment-min 6 --increment-max 8 ?h?h?h?h?h?h?h?h
h?h?h

自定义掩码规则:

```
--custom-charset1 [chars]等价于 -1  
--custom-charset2 [chars]等价于 -2  
--custom-charset3 [chars]等价于 -3  
--custom-charset4 [chars]等价于 -4
```

在掩码中用 ?1、?2、?3、?4 来表示

注意:

- --custom-charset1 abcd ?1?1?1?1?1 等价于 -1 abcd ?1?1?1?1?1
- -3 abcdef -4 123456 ?3?3?3?3?4?4?4?4 表示前四位可能是 adbcdef, 后四位可能是 123456

另外 Hash 模式与 ID 的对照表由于太长, 这里就不放了, 可以直接 hashcat -h 进行查看

示例

MD5

密码为 8 位数字

```
hashcat -a 3 --force d54d1702ad0f8326224b817c796763c9 ?d?d?d?d?d?d?d?d
```

密码为 4 位小写字母+数字

```
hashcat -a 3 --force 4575621b0d88c303998e63fc74d165b0 -1 ?l?d ?l?l?l?l?l
```

密码为 1-4 位大写字母+数字

```
hashcat -a 3 --force 8fb5a3e7338ce951971d69be27fc5210 -1 ?u?d ?l?l?l?l?l --  
increment --increment-min 1 --increment-max 4
```

指定特定字符集: 123456abcdf!@+- 进行破解

```
hashcat -a 3 -1 123456abcdf!@+- 8b78ba5089b11326290bc15cf0b9a07d ?l?l?l?l?l?l
```

由于在终端里可能会把部分字符识别为特殊字符, 因此需要转义一下

```
hashcat -a 3 -1 123456abcdf\!\@+- 8b78ba5089b11326290bc15cf0b9a07d ?l?l?l?l?l?l
```

如果不知道目标密码的构成情况, 可以直接使用 ?a 表示使用所有字符进行破解

```
hashcat -a 3 19b9a36f0cab6d89cd4d3c21b2aa15be --increment --increment-min 1 --increment-max 8 ?a?a?a?a?a?a?a
```

使用字典破解

```
hashcat -a 0 e10adc3949ba59abbe56e057f20f883e password.txt
```

使用字典批量破解

```
hashcat -a 0 hash.txt password.txt
```

字典组合破解

```
hashcat -a 1 77b3e6926e7295494dd3be91c6934899 pwd1.txt pwd2.txt
```

经过测试，这里的字典组合破解，不是说简单的将两个字典的内容合并去重形成 1 个字典进行去重，而是说字典 1 的内容加上字典 2 的内容组合成一个字典，例如：

pwd1.txt 字典为：

```
admin
test
root
```

pwd2.txt 字典为：

```
@2021
123
```

那么组合后的字典就是这样的：

```
admin@2021
admin123
test@2021
test123
root@2021
root123
```

字典+掩码破解，也是和上面一样的组合方法，只不过 pwd2.txt 换成了掩码

```
hashcat -a 6 e120ea280aa50693d5568d0071456460 pwd1.txt ?l?l?l
```

Mysql4.1/5

```
hashcat -a 3 -m 300 --force 6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 ?d?d?d?d?d?d
```

可以使用 `select authentication_string from mysql.user;` 查看当前数据库中的密码哈希值。

sha512crypt \$6\$, SHA512 (Unix)

sha512crypt \$6\$, SHA512 (Unix) 破解，为了避免系统误识别到特殊字符，这里为哈希值加了单引号

```
hashcat -a 3 -m 1800 --force  
'$6$mxuA5cdy$XZRk0CvnPFqOgVopqiPEFAFK72SogKVwwwp7gwaUOb7b6tVwfCpcSusCEk64ktLLYmz  
yew/xd00hPG/ym2X.' ?1?1?1?1
```

可通过 `cat /etc/shadow` 获取哈希值

或者不删除用户名，直接使用 `--username` 参数

```
hashcat -a 3 -m 1800 --force  
'qiyou:$6$QDq75ki3$jskm7qTDHz/xBob0kF1Lp170Cgg0i5Ts1f3Jw/sm9k9Q916mBTyi1u3PoOsbr  
dxv8TAMzvdgNjrcuhfg3jKMY1' ?1?1?1?1?1 --username
```

NTLM

NT Hash

```
hashcat -a 3 -m 1000 209C6174DA490CAEB422F3FA5A7AE634 ?1?1?1?1?1
```

LM Hash

```
hashcat -a 3 -m 3000 F0D412BD764FFE81AAD3B435B51404EE ?1?1?1?1?1
```

NetNTLM Hash

```
hashcat -a 3 -m 5500  
teams.six::::822795daaf96s0a811fs6dd7b01dscssc601635cc1339basda6:e125cddcf51337a  
sc7 -1 ?1?u ?1?1?1?1?d?d?d?d --force
```

MSSQL (2005)

```
hashcat -a 3 -m 132 --force  
0x01008c8006c224f71f6bf0036f78d863c3c4ff53f8c3c48edafb ?1?1?1?1?1?d?d?d
```

WordPress 密码 hash

```
hashcat -a 3 -m 400 --force '$P$BYEYCHEj3vDhV1lwGBv6rpxurKOEWY/' ?d?d?d?d?d?d
```

具体加密脚本在 `./wp-includes/class-phpass.php` 的 `HashPassword` 函数

Discuz 用户密码 hash

```
hashcat -a 3 -m 2611 --force 14e1b600b1fd579f47433b88e8d85291: ?d?d?d?d?d?d
```

其密码加密方式 `md5(md5($pass).$salt)`

RAR 压缩密码

首先获取 rar 文件的 hash 值，我们可以使用另一款哈希破解工具 John 提供的 `rar2john` 工具将 rar 文件里的 hash 提取出来。

rar2john 下载地址: <http://openwall.info/wiki/media/john/johntheripper-v1.8.0.12-jumbo-1-bleeding-e6214ceab-2018-02-07-win-x64.7z>

```
# 获取 rar 文件 hash
rar2john.exe 1.rar
```

hashcat 支持 RAR3-hp 和 RAR5

对于 RAR5, 示例如下:

```
hashcat -a 3 -m 13000 --force
'$rar5$16$b06f5f2d4c973d6235e1a88b8d5dd594$15$a520dddc53dd4e3930b8489b013f273$8
$733969e5bda903e4' ?d?d?d?d?d
```

对于 RAR3-hp

```
hashcat -a 3 -m 12500 --force
'$RAR3$*0*5ba3dd697a8706fa*919ad1d7a1c42bae4a8d462c8537c9cb' ?d?d?d?d
```

RAR3-hp 哈希头为 \$RAR3\$0, 而不是 \$RAR3\$1, 中间的数值是0 (-hp) 而不是1 (-p), -p 尚未得到支持, 只支持 -hp

关于 RAR 参数 -p 和 -hp 的区别: -p: 只对 RAR 文件加密, 里面的目录和文件名没加密; -hp: 对目录中的文件名和子目录都进行加密处理

ZIP 压缩密码

和 rar 破解过程一样, 我们需要先提取 zip 文件的哈希值, 这里可以使用 zip2john 进行获取, zip2john.exe 在上面下载的 rar2john.exe 的同级目录下。

```
# 获取 zip 文件 hash
zip2john.exe 1.zip
hashcat -a 3 -m 13600
'$zip2$*0*3*0*18b1a7e7ad39cb3624e54622849b23c7*5b99*3*5deee7*a418cee1a98710adce9
a*$zip2$' --force ?d?d?d?d?d
```

这里 ZIP 的加密算法使用的 AES256

office 密码

和 rar 与 zip 破解过程一样, 我们需要先提取 office 文件的哈希值, 这里可以使用 office2john.py 进行获取, office2john.py 在上面下载的 rar2john.exe 和 zip2john.exe 的同级目录下。

```
# 获取 office 文件 hash
python office2john.py 1.docx
```

测试中发现 python 会出现告警信息, 不过这个告警信息不会影响程序执行

```
hashcat -a 3 -m 9600
'$office$*2013*100000*256*16*cd8856416b1e14305a0e8aa8eba6ce5c*18cada7070f1410f3a
836c0dfc4b9643*befcde69afeafb3e652719533c824413b00ce4a499589e5ac5bd7a7a0d3c4f3d'
--force ?d?d?d?d?d
```

这里哈希头为 2013 所以使用 9600 破解模式，如果是 2010 则使用 9500 破解模式，2007 则使用 9400 破解模式。

WIFI 密码

要破解 WIFI 密码，首先要抓到 WIFI 的握手包，要想得到 WIFI 的握手包，就需要在监听时刚好有设备连接了该 WIFI，但这就需要运气加成，因此我们可以主动将该 WIFI 的设备踢下去，一般设备就会自动连接该 WIFI，此时我们就抓到握手包了。

抓取 WIFI 握手包

1、将网卡处于监听状态

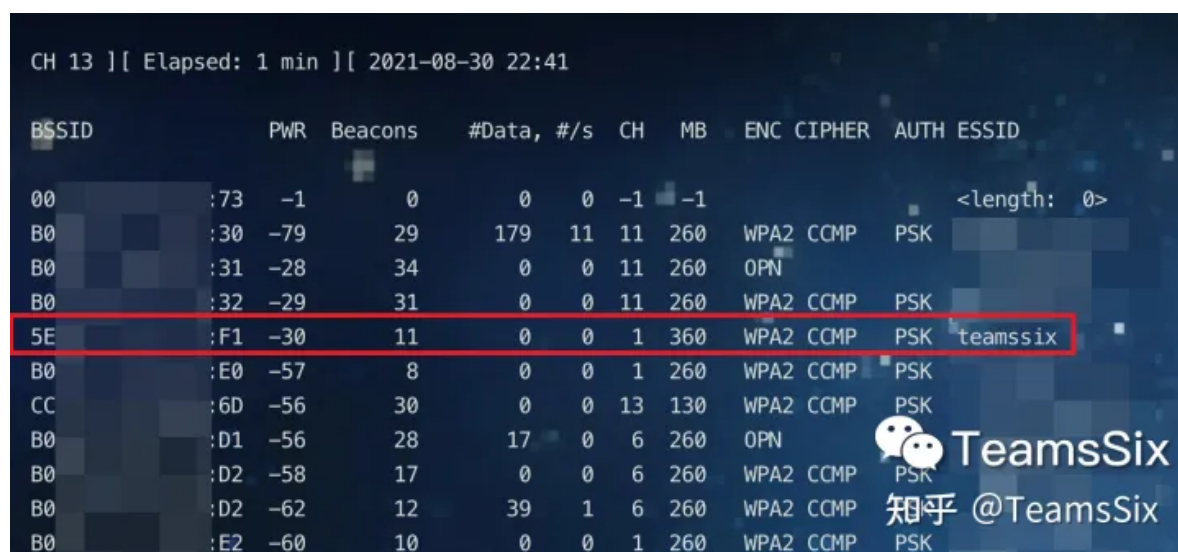
```
airmon-ng check
airmon-ng check kill // 关闭影响监听状态的进程
airmon-ng start wlan0
```

wlan0 是网卡名称，一般都是 wlan0，如果不是则需要根据自己的情况进行修改，可通过 iwconfig 进行查看网卡的名称

当使用 iwconfig 查看网卡名称变为 wlan0mon 说明此时网卡已经处于监听模式了

2、扫描可用 WIFI

```
airodump-ng wlan0mon
```



BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:73:30	-1	0	0 0	-1	-1				<length: 0>
B0:30	-79	29	179 11	11	260	WPA2	CCMP	PSK	
B0:31	-28	34	0 0	11	260	OPN			
B0:32	-29	31	0 0	11	260	WPA2	CCMP	PSK	
5E:C1:1B:A2:37:F1	-30	11	0 0	1	360	WPA2	CCMP	PSK	teamssix
B0:E0	-57	8	0 0	1	260	WPA2	CCMP	PSK	
CC:6D	-56	30	0 0	13	130	WPA2	CCMP	PSK	
B0:D1	-56	28	17 0	6	260	OPN			
B0:D2	-58	17	0 0	6	260	WPA2	CCMP	PSK	
B0:D2	-62	12	39 1	6	260	WPA2	CCMP	PSK	
B0:E2	-60	10	0 0	1	260	WPA2	CCMP	PSK	

3、获取wifi的握手包

```
airodump-ng -c (上一步扫描的 CH) --bssid (想要破解 WIFI 的 bssid) -w (握手文件存放目录) wlan0mon
```

这里以 ssid 为 teamssix 的 WIFI 为例

```
airodump-ng -c 1 --bssid 5E:C1:1B:A2:37:F1 -w ./ wlan0mon
```

为了顺利得到 WIFI 的握手包，可以将该 WIFI 下的设备强制踢下去

```
aireplay-ng -0 0 -a (要破解的 wifi 的 bssid) -c (强制踢下的设备的 MAC 地址) wlan0mon
```

```
CH 1 ][ Elapsed: 2 mins ][ 2021-08-30 22:53

BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
5E:1B:A2:37:F1 F1 -33 90      900      16   0  1  360 WPA2 CCMP PSK teamssix

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
5E:1B:A2:37:F1 38:26:2C:13:D3:33 -30  1e-24e  9    322    知乎 @TeamsSix
```

可以看到 teamssix 这个 WIFI 有一个设备正在连接，该设备的 MAC 地址为：38:26:2C:13:D3:33，使用以下命令可以将其强制踢下去

```
aireplay-ng -0 0 -a 5E:C1:1B:A2:37:F1 -c 38:26:2C:13:D3:33 wlan0mon
```

等待设备重新连接后，当右上角出现 WPA handshake 的时候说明获取成功

```
CH 1 ][ Elapsed: 54 s ][ 2021-08-30 22:59 ][ WPA handshake: 5E:1B:A2:37:F1

BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
5E:1B:A2:37:F1 F1 -31 87      373      42   0  1  360 WPA2 CCMP PSK teamssix

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
5E:1B:A2:37:F1 38:26:2C:13:D3:33 -32  1e-24e  75    516 EAPOL 知乎 @TeamsSix
```

4、破解密码

使用 aircrack-ng 将握手包转换成 hccapx 格式

```
aircrack-ng 1.cap -j 1
hashcat -a 3 -m 2500 1.hccapx ?d?d?d?d?d?d?d?d --force
```

或者使用 hashcat 官网提供的在线工具进行格式转换：<https://hashcat.net/cap2hashcat/>

```
hashcat -a 3 -m 22000 1.hc22000 ?d?d?d?d?d?d?d?d --force
```


Host memory required for this attack: 602 MB

66c6f9582642e5b6f2bac28752bb1f83:5ebf6bdc57f1:38378b91b933:teamssix:11111112

Session.....: hashcat

Status.....: Cracked

Hash.Name.....: WPA-PBKDF2-PMKID+EAPOL

Hash.Target.....: 1.hc22000

Time.Started.....: Tue Aug 31 11:32:10 2021, (32 secs)

Time.Estimated...: Tue Aug 31 11:32:42 2021, (0 secs)

Guess.Mask.....: ?d?d?d?d?d?d?d [8]

Guess.Queue.....: 1/1 (100.00%)

Speed.#2.....: 6921 H/s (6.50ms) @ Accel:64 Loops:16 Thr:8 Vec:1

Speed.#3.....: 94832 H/s (6.57ms) @ Accel:8 Loops:256 Thr:64 Vec:1

Speed.*.....: 101.8 kH/s

Recovered.....: 1/1 (100.00%) Digests

Progress.....: 3170304/100000000 (3.17%)

Rejected.....: 0/3170304 (0.00%)

Restore.Point....: 12288/100000000 (0.12%)

Restore.Sub.#2...: Salt:0 Amplifier:7-8 Iteration:

Restore.Sub.#3...: Salt:0 Amplifier:0-1 Iteration:0-1

Candidates.#2....: 82192712 -> 83044988

Candidates.#3....: 16826612 -> 15968612



TeamsSix

知乎 @TeamsSix

5、其他

- Hashcat 在有时破解的时候会提示 All hashes found in potfile!, 这表明该 hash 已经被破解出来了, 可以使用 hashcat [哈希值] --show 查看已破解出来的明文密码。
- 如果想再次破解已经破解过的密码, 删除 ~/.hashcat/hashcat.potfile 文件里的对应记录即可。
- 在使用GPU模式进行破解时, 可以使用 -O 参数自动进行优化
- 在实际破解过程中, 可以先使用 top 字典进行破解, 不行再试试社工字典, 比如姓名+生日的组合字典
- Hashcat 参数优化:

--gpu-accel 160	可以让GPU发挥最大性能
--gpu-loops 1024	可以让GPU发挥最大性能
--segment-size 512	可以提高大字典破解的速度