hashcat详细使用教程

原创 星落. 2020-05-14 11:00:11 23468 收藏 18 版权

分类专栏： Kali工具使用教程 文章标签： hashcat

hashcat简介

hashcat是一款自称为世界上最快的密码破解工具。

hashcat常用命令

-m	指定哈希类型
-a	指定破解模式
-V	查看版本信息
-o	将输出结果储存到指定文件
--force	忽略警告
--show	仅显示破解的hash密码和对应的明文
--remove	从源文件中删除破解成功的hash
--username	忽略hash表中的用户名
-b	测试计算机破解速度和相关硬件信息
-O	限制密码长度
-T	设置线程数
-r	使用规则文件
-1	自定义字符集 -1 0123asd ?1={0123asd}
-2	自定义字符集 -2 0123asd ?2={0123asd}
-3	自定义字符集 -3 0123asd ?3={0123asd}
-i	启用增量破解模式
--increment-min	设置密码最小长度
--increment-max	设置密码最大长度

hashcat破解模式介绍

0	straight	字典破解
1	combination	将字典中密码进行组合（1 2>11 22 12 21）
3	brute-force	使用指定掩码破解
6	Hybrid Wordlist + Mask	字典+掩码破解
7	Hybrid Mask + Wordlist	掩码+字典破解

hashcat集成的字符集

?l	代表小写字母
?u	代表大写字母
?d	代表数字
?s	代表特殊字符

?a 代表大小写字母、数字以及特殊字符

?b 0x00-0xff

hash id 对照表

900	MD4	Raw Hash
0	MD5	Raw Hash
5100	Half MD5	Raw Hash
100	SHA1	Raw Hash
1300	SHA2-224	Raw Hash
1400	SHA2-256	Raw Hash
10800	SHA2-384	Raw Hash
1700	SHA2-512	Raw Hash
17300	SHA3-224	Raw Hash
17400	SHA3-256	Raw Hash
17500	SHA3-384	Raw Hash
17600	SHA3-512	Raw Hash
17700	Keccak-224	Raw Hash
17800	Keccak-256	Raw Hash
17900	Keccak-384	Raw Hash
18000	Keccak-512	Raw Hash
600	BLAKE2b-512	Raw Hash
10100	SipHash	Raw Hash
6000	RIPEMD-160	Raw Hash
6100	Whirlpool	Raw Hash
6900	GOST R 34.11-94	Raw Hash
11700	GOST R 34.11-2012 (Streebog) 256-bit, big-endian	Raw Hash
11800	GOST R 34.11-2012 (Streebog) 512-bit, big-endian	Raw Hash
10	md5($pass.$salt)	Raw Hash, Salted and/or Iterated
20	md5($salt.$pass)	Raw Hash, Salted and/or Iterated
30	md5(utf16le($pass).$salt)	Raw Hash, Salted and/or Iterated
40	md5($salt.utf16le($pass))	Raw Hash, Salted and/or Iterated
3800	md5($salt.$pass.$salt)	Raw Hash, Salted and/or Iterated
3710	md5($salt.md5($pass))	Raw Hash, Salted and/or Iterated
4010	md5($salt.md5($salt.$pass))	Raw Hash, Salted and/or Iterated
4110	md5($salt.md5($pass.$salt))	Raw Hash, Salted and/or Iterated
2600	md5(md5($pass))	Raw Hash, Salted and/or Iterated
3910	md5(md5($pass).md5($salt))	Raw Hash, Salted and/or Iterated
4300	md5(strtoupper(md5($pass)))	Raw Hash, Salted and/or Iterated
4400	md5(sha1($pass))	Raw Hash, Salted and/or Iterated
110	sha1($pass.$salt)	Raw Hash, Salted and/or Iterated

实例演示-暴力破解MD5值

1.使用字典进行破解

hashcat -a 0 0192023a7bbd73250516f069df18b500 password.txt --force

```
root@kali:~# hashcat  0192023a7bbd73250516f069df18b500  -a 0  password.txt --force
hashcat (v5.1.0) starting...

OpenCL Platform #1: The pocl project
====================================
* Device #1: pthread-Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz, 1024/2954 MB allocatable, 6MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

* Device #1: build_opts '-cl-std=CL1.2 -I OpenCL -I /usr/share/hashcat/OpenCL -D LOCAL_MEM_TYPE=2 -D VENDOR_ID=64 -D CUDA_ARCH=0 -D AMD_ROCM=0 -D VECT_SIZE=8 -D DEVICE_TYPE=2 -D DGST_R0=0 -D DGST_R1=3 -D DGST_R2=2 -D DGST_R3=1 -D DGST_ELEM=4 -D KERN_TYPE=0 -D _unroll'
Dictionary cache hit:
* Filename..: password.txt
* Passwords.: 32
* Bytes.....: 137
* Keyspace..: 32

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

0192023a7bbd73250516f069df18b500:admin123

Session..........: hashcat
Status...........: Cracked
Hash.Type........: MD5
Hash.Target......: 0192023a7bbd73250516f069df18b500
Time.Started.....: Wed May 13 22:15:53 2020 (1 sec)
Time.Estimated...: Wed May 13 22:15:54 2020 (0 secs)
Guess.Base.......: File (password.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      259 H/s (0.01ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 32/32 (100.00%)
Rejected.........: 0/32 (0.00%)
Restore.Point....: 0/32 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: → 123
```

2.使用指定字符集进行破解

hashcat -a 3 63a9f0ea7bb98050796b649e85481845 ?l?l?l?l --force

```
root@kali:~# hashcat  63a9f0ea7bb98050796b649e85481845  -a 3 ?l?l?l?l --force
hashcat (v5.1.0) starting...

OpenCL Platform #1: The pocl project
====================================
* Device #1: pthread-Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz, 1024/2954 MB allocatable, 6MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Brute-Force
* Raw-Hash

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

* Device #1: build_opts '-cl-std=CL1.2 -I OpenCL -I /usr/share/hashcat/OpenCL -D LOCAL_MEM_TYPE=2 -D VENDOR_ID=64 -D CUDA_ARCH=0 -D AMD_ROCM=0 -D VECT_SIZ
E=8 -D DEVICE_TYPE=2 -D DGST_R0=0 -D DGST_R1=3 -D DGST_R2=2 -D DGST_R3=1 -D DGST_ELEM=4 -D KERN_TYPE=0 -D _unroll'
* Device #1: Kernel m00000_a3-pure.34167de1.kernel not found in cache! Building may take a while...
* Device #1: Kernel markov_le.f6324eeb.kernel not found in cache! Building may take a while...
63a9f0ea7bb98050796b649e85481845:root

Session..........: hashcat
Status...........: Cracked
Hash.Type........: MD5
Hash.Target......: 63a9f0ea7bb98050796b649e85481845
Time.Started.....: Wed May 13 22:33:12 2020 (0 secs)
Time.Estimated...: Wed May 13 22:33:12 2020 (0 secs)
Guess.Mask.......: ?l?l?l?l [4]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   428.8 kH/s (2.02ms) @ Accel:1024 Loops:26 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 159744/456976 (34.96%)
Rejected.........: 0/159744 (0.00%)
Restore.Point....: 0/17576 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-26 Iteration:0-26
Candidates.#1....: sari -> xhir

Started: Wed May 13 22:32:33 2020
Stopped: Wed May 13 22:33:13 2020
root@kali:~#
```

你的浏览器目前处于缩放状态，页面可能会出现错位现象，建议100%大小显示。

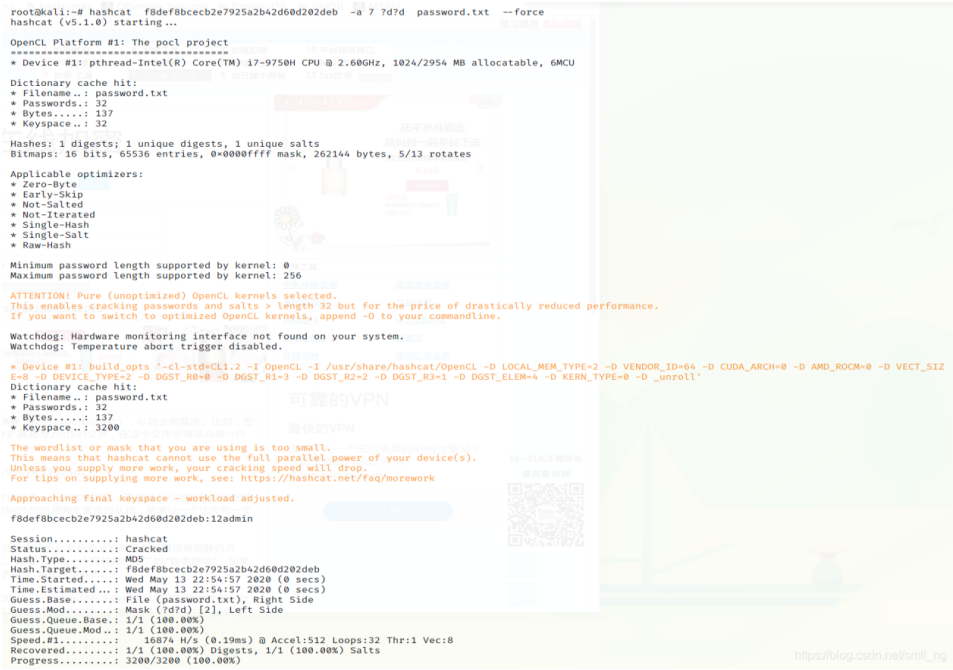
3.使用字典+掩码进行破解

hashcat -a 6 1844156d4166d94387f1a4ad031ca5fa password.txt ?d?d?d --force

```
root@kali:~# hashcat  1844156d4166d94387f1a4ad031ca5fa  -a 6  password.txt ?d?d --force
hashcat (v5.1.0) starting...

OpenCL Platform #1: The pocl project
====================================
* Device #1: pthread-Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz, 1024/2954 MB allocatable, 6MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

* Device #1: build_opts '-cl-std=CL1.2 -I OpenCL -I /usr/share/hashcat/OpenCL -D LOCAL_MEM_TYPE=2 -D VENDOR_ID=64 -D CUDA_ARCH=0 -D AMD_ROCM=0 -D VECT_SIZ
E=8 -D DEVICE_TYPE=2 -D DGST_R0=0 -D DGST_R1=3 -D DGST_R2=2 -D DGST_R3=1 -D DGST_ELEM=4 -D KERN_TYPE=0 -D _unroll'
Dictionary cache built:
* Filename..: password.txt
* Passwords.: 32
* Bytes.....: 137
* Keyspace..: 3200
* Runtime...: 0 secs

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

1844156d4166d94387f1a4ad031ca5fa:admin12

Session..........: hashcat
Status...........: Cracked
Hash.Type........: MD5
Hash.Target......: 1844156d4166d94387f1a4ad031ca5fa
Time.Started.....: Wed May 13 22:44:39 2020 (0 secs)
Time.Estimated...: Wed May 13 22:44:39 2020 (0 secs)
Guess.Base.......: File (password.txt), Left Side
Guess.Mod........: Mask (?d?d) [2], Right Side
Guess.Queue.Base.: 1/1 (100.00%)
Guess.Queue.Mod..: 1/1 (100.00%)
Speed.#1.........:     9565 H/s (0.18ms) @ Accel:256 Loops:100 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 3200/3200 (100.00%)
Rejected.........: 0/3200 (0.00%)
Restore.Point....: 0/32 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-100 Iteration:0-100
```

4.使用掩码+字典进行破解

hashcat -a 7 f8def8bcecb2e7925a2b42d60d202deb ?d?d password.txt --force



如果破解时间太长，我们可以按s键查看破解进度，p键暂停，r键继续破解，q键退出破解。

到此就完成了hashcat的介绍，如果想了解更多的Kali工具，请关注我！

hashcat-4.1.0.7_hashcat软件下载,hashcat下载-其它工具类资源... 12-17
当前最强大的开源密码恢复工具,你可以访问Hashcat.net网站来了解这款工具的详细情况。本质上,Hashcat 3.0是…

hashcat的一点密码破解的心得（转载） 03-04
hashcat的命令行详解，真正高手必备。

hashcat的前世今生 测试 334
目录 hashcat的前世今生1. Hashcat组件发展简史1.1. Hashcat1.2. OclHahcat hashcat的前世今生 hashcat 号称世…

星落.
码龄1年 哈尔滨理工大学

67	9125	1万+	81万+	
原创	周排名	总排名	访问	等级
5331	123	88	25	315
积分	粉丝	获赞	评论	收藏

私信 关注

搜博主文章

热门文章

分类专栏

最新评论

Shodan详细使用教程
wowo147258: shodan高级会员 20万查询分获取海量数据 https://item.taobao.com/it …

Maltego详细使用教程
whylon: 用谷歌浏览器

Maltego详细使用教程
痕夕大爹: 登录也得翻墙吗，我之前上油管的号这个也可以登吗

BeEF-XSS详细使用教程
液冷: 没事了没事了

最新文章

CVE-2018-12613| phpmyadmin远程文件包含漏洞

Apache多后缀名解析漏洞

CVE-2020-14882 WebLogic远程代码执行漏洞

2020

12月	11月	10月	09月
3篇	3篇	2篇	4篇
07月	06月	05月	
1篇	13篇	41篇	

目录