Cracking WEP Encrypted 802.11 Networks: A Beginner's Guide
by Tristan Mendoza

Backtrack2 is a very nice Linux distribution with a security audit focus available at the Remote-Exploit.org website. Here is where to download the ISO file so you can burn it to a cd. You won't regret having it around, and it will be used exclusively in this tutorial.
http://www.remote-exploit.org/backtrack.html

[For this example, you will be asked to put in the appropriate data for the networks and devices in your use of these instructions. For this example, `rausb0` is my network adapter, `2WIREXXX` is the AP's (access point's) name or SSID and it's BSSID/MAC address is `00:EE:E4:A7:0E:EE` - you will need to replace these with the information in your scenario]

Getting Started
1) Boot off of Backtrack2 CD. When you get a prompt, remember to run xconf before running startx.

2) Open up a terminal: type "`iwconfig`" and look for your adapter listed. If you see it and you dont see it marked as saying it is in Monitor Mode, type "`iwconfig rausb0 mode monitor`" after doing so type: "`airmon-ng start rausb0`" (this double-checks)

troubleshooting tip
If iwconfig sees the wireless adapter, but returns this error when mode set is entered:
`Error for wireless request "Set Mode (8B06) SET failed on device RAUSB0 network is down"`
(Airmon also displays no devices in this instance) Type the following series of commands to fix it:

```
>airmon-ng stop rausb0
>ifconfig rausb0 down
>ifconfig rausb0 up
>airmon-ng start rausb0
```

Setting Up: Intelligence Gathering
3) In the same terminal that was already open, type "`airodump-ng rausb0`" Airodump-ng is used by many to grab packets, but we are going to use Kismet later for that task. Typing the command above will display a list of the wireless networks on top that are available, and some information on each. Also, watch this screen for a client machine's MAC address to be listed in bottom list (next to that computer's MAC address will be the access point). Leave this window open as reference, since these values will update.

4) In a new terminal window, type "kismet" to open Kismet. Up comes a list of what it finds, that you can sort by pressing "s" You can select a network in the list and type "i" to get to an info screen. Client machines can be viewed by pressing "c" (an alternative to the view airodump-ng gives us), and when we do the actually capturing of packets soon, we'll type L to limit handling to the channel that network resides on. Type "q" if you seem stuck and have trouble getting back to the main screen.

Choosing a Network
After viewing Kismet and Airodump-ng, you can see which AP's (access points) have a stronger signal, what sortof encryption they are using (if any), and some other information that is useful, like what channel they are broadcasting on, and if we see any clients connected to them. You want a network that has a strong signal, is showing as WEP encryted, and it is nice- but not necessary- to have a network which isn't sharing a channel with other networks. It also helps, but is not necessary, to have clients connected so that you can use their MAC addresses later.

We are going to close Kismet for now (ctrl-c), but first you should write down the name of the network, and the MAC address (listed as the BSSID). If you see a connected client's MAC address (meaning it's associated BSSID matches the AP you want to work on) you will want to write it down too.

Setting Up: Getting Tools Ready

5) In this step, we will open up 3 new terminal windows that will be used to properly do the gathering of the packets that we need. I suggest using the second virtual desktop pane to hold these. For right now, DO NOT press return in these terminals- simply input the command lines for them, and we will just start them off all at once at the end. Remember- we are just laying out our tools, so don't hit return yet.

a) The first terminal window is going to be our ARPReplay window. Since we aren't going to be capturing the ARP packets it works with using aerodump-ng, it may not seem necessary, though I get the feeling it helps to have it running. Type the following, and *DO NOT HIT RETURN YET*.

```
>aireplay-ng rausb0 --arpreplay -e 2WIREXXX -b 00:EE:E4:A7:0E:EE -h [client machine MAC]
```

b) The second terminal will perform the deauthentication flood necessary to speed up packet broadcasts from the AP. Below, the 100 is the number of times it should send. During the capture, you will be running this command over and over until you have enough IV's to get the WEP key. In this terminal, type the following, and *DO NOT HIT RETURN YET.*

```
>aireplay-ng rausb0 --deauth 100 -a 00:EE:E4:A7:0E:EE -c [client machine MAC]
```

c) The third terminal window we need is going to send fake authentications for us. Unlike the deauthication flood, in window 2, this runs only once at a time. It will report "waiting for beacon frame", "sending authentication request", "authentication successful", "sending association request", and "association successful" in that order and quit. I like to alternate this and the deauthentication attack, or if I really get bored, run them simultaneously and let the router fight with itself. Type in the following *and DO NOT HIT RETURN YET*.

```
>aireplay-ng -1 0 -a 00:EE:E4:A7:0E:EE -h [client machine MAC] rausb0
```

Note: with these commands, the "-h" and "-c" options are generally intended to be for listing the MAC address for one of the client computers connected to the AP. Don't have one from before? No problem! Either use your MAC address or try to use a fake one. I was doing this on a computer I wont be surfing with so I just put in the USB adapter's MAC address without giving it thought.

Precracking the WEP Key: Packet Harvesting

Now that we have our tools ready to run in the 3 terminal windows we just opened, it's time to double check that everything is all set. Do all of the numbers match (no typos)? Ok, time to get some data to crack this open with.

6) Follow these steps:

a) Reopen kismet as we did earlier in a new terminal. With the AP's listed, press "s" to sort, and sort them by channel.

b) Choose the target AP with the arrow keys, and when highlighted, type "L." The notes at the bottom should confirm that Kismet has locked onto only the channel that AP is broadcasting on. These are the packets that Kismet will through in the .dump file

c) Press return in the 3 terminal windows we opened in step 5. Looking to Kismet to eyeball our AP's status, notice the numbers in the field #data start increasing much faster than they were in response to our activities. This also shows in the ARPReplay window.

7) Ok, so if this is all working as it should we are sortof at the boring part. Monitor your progress in Kismet, and keep the deauthentication and fake authentications running (at least one or the other) repeatedly. You will probably notice that one of the two works better to make packet collection go faster, so alternate and use the one you think works better more often- I alternate them.

8) When to stop? Notice that in Kismet, there are some numbers displayed to the side in a small panel to the top right in the main window. You want to keep your eye on the AP's column for #data, but what is really important is listed in the far right portion under "crypt." This is how many encrypted packets- the ones we need- Kismet has saved to the dump file so far. It is said that for a 64-bit key, we will need a minimum of 500,000 IV's and for a 128-bit, we need at least 1 million. When this crypt # gets in this neighborhood (I like having a bit more than recommended), we can move on to the next step.

9) Do we have enough packets yet?? Let's find out. Backtrack2 uses Konquerer as a file browser, so open that, and go to your home directory.

a) There, find Kismet's file which ends in .dump and be sure it is the latest one.

b) Copy this file, and paste it with the name changed (don't overwrite the existing one!) -change the extension ".dump" to ".cap"

c) Open a new terminal and type in "`aircrack-ng -n 64 capturefile.cap`" where capturefile.cap is the same name as your renamed dump file. The "-n 64" part is optional. Starting with it when you have enough packets for 64 bit can be a test to see if you even need to gather more packets.

d) Aircrack will present us with a list of access points, and a number of IV packets we have so far for each one. This is the authoritative number that you use to determine if you have enough packets (500,000 for 64bit, 1 million for 128bit).

e) If you are ready, select your target AP and hit return. If it takes more than 15 minutes, cancel out (ctrl-c) to start over. If it just told you that you had over 500,000 IVs, (but under 1 million) then you can run it again changing what it calls the "fudge factor." The fudge factor is sortof the degree of random sloppiness that Aircrack uses in determining the key. We just ran it using the normal factor of 4, so if you type "`aircrack-ng -n 64 -f 8 capturefile.cap`" this will make it a factor of 8. Try this for 15 minutes, and if it doesn't work, go to f=12 for a while. If this still doesn't work, there is a good chance that you have a 128-bit network. Go ahead and trash the temporary copy we made of the capture file (named .cap). We will get more packets (since Kismet, deauth and auth windows are still going) and try it when we have over a million IVs.

10) When we think Kismet has over 1 million packets collected, repeat step 9. If Aircrack tells you right up front you don't have over 1 million- you will need to capture more and try again. This time we are going to run Aircrack without specifying the bits, the -n 64 part and we are also going to start back without specifying a fudge factor (just typing "`aircrack-ng capturefile.cap`"). This should NOT take long. If you wait 20 minutes and still nothing, then cancel it and start it with a higher fudge factor.

Eventually it will spit out the hex key for the WEP, and will often give you the string. If you have increased the fudge factor as high as 15 and it is still taking over 1/2 hour, perhaps consider this a dry run and try all of this later. More packets always help... Did you quit Kismet? If it has been capturing still even now, then you could try to get more packets. I like to get about 1.5 million if it proves not to be a 64-bit key, although I ran the first successful go at this at 6pm or so, aircrack got the 128-bit in about 15 seconds, 1,031,481 IVs, 57 keys tested) about 8pm.

Websites to Check Out

http://www.kismetwireless.org
http://www.aircrack-ng.org
http://forums.remote-exploit.org/