

Forum:[Hack Forums](#)

Thread: [\[My Vid Tut\] How to crack WEP Keys on Backtrack 100%](#)

Ralph_Lauren - March 17, 2012, 11:45 am

Hello HF I am releasing my first tutorial that I made on Youtube and I wanted to share it with you guys. It's my first tutorial so please bare with me. This will show you how to crack wep encrypted networks through Backtrack. Please tell me what you think, I am open for any constructive criticism. If you have any questions feel free to PM me :) Thanks!

Ralph_Lauren - March 25, 2012, 4:04 pm

Has nobody looked at my tutorial :(
Im so sad

Sights101 - March 25, 2012, 6:02 pm

I've looked at it. It's a very nice tutorial. I suggest copying the word document into the thread.

Ralph_Lauren - March 25, 2012, 8:18 pm

(Mar 25, 2012 06:02 PM)Sights101 Wrote: [\[CITE\]](#) I've looked at it. It's a very nice tutorial. I suggest copying the word document into the thread.

Thanks for your feedback it is greatly appreciated :)

And I will put the instruction on this thread when I have time

D Generation X - March 26, 2012, 2:19 am

nice tut mate..great job keep it up

Ralph_Lauren - March 26, 2012, 2:02 pm

Thanks! Glad you liked it. I will be posting some more
in the future

Jiujitsu - March 28, 2012, 10:23 am

Good video I will have to try this. The intro should be shortened by like 5 seconds.

Ralph_Lauren - March 28, 2012, 1:12 pm

(Mar 28, 2012 10:23 AM)Jiujitsu Wrote: [\[CITE\]](#) Good video I will have to try this. The intro should be shortened by like 5 seconds.

Yea lol your right.

I was just in a hurry to get it online

conrad - March 30, 2012, 4:39 pm

Great tutorial but I seem to be having trouble with capturing process. My system becomes very slow, so far #700 has taken 30mins.

I running:

vmware workstation

backtrack 5r2, 1028 ram, 1 processor, 50gb virtual hd

Netbook:
Atom n550 dual core 1.6
2 gb ram
Alfa Network AWUS036H

Is there anything that would speed it up?

Ralph_Lauren - March 30, 2012, 4:57 pm

Hmm by default your AWUS036H doesn't come with its full range capacity for legal reasons.

Some countries have a specific amount of range that they only allow.

Type this in the console to increase your adapter to its full range

```
root@bt:~# ifconfig wlan0 down
```

```
root@bt:~# iw reg set US
```

```
root@bt:~# airmon-ng start wlan0
```

(Then some description about your adapter should show up, then just type the following:)

```
root@bt:~# iwconfig wlan0
```

(Now you should see your adapter's information, and somewhere in there it should say

"Tx-Power=30 dbm") <-- 30 dbm means success. Mine usually reaches 27 dbm and that's ok. Tell me if I helped you :)

Note: You have to type this in every time you turn on your VMWare

beba - March 30, 2012, 9:12 pm

can this tut be done in backtrack 4

Ralph_Lauren - March 30, 2012, 9:16 pm

I'm pretty sure, try it either way, you don't have anything to lose

ryck - March 30, 2012, 11:41 pm

Great job dude, absolutely perfect job, thanks for sharing. That was really useful tutorial. I hope you make more tutorials like this one. Respect.

Ralph_Lauren - March 31, 2012, 12:07 am

Thanks bro hope you liked it :)

And yes I will in the future

imrankhan - March 31, 2012, 1:56 am

what is it 4 lol

what can you do with the WEP

i am a beginner lol

Ralph_Lauren - March 31, 2012, 7:41 am

Once you have their wep password, you can get on their internet
or you can enter into a hijacking session

imrankhan - March 31, 2012, 8:55 am

could you make another tutorial about "hijacking session"

could you make another tutorial about "hijacking session"

Ralph_Lauren - March 31, 2012, 9:38 am

Yes I will when I have time

Don't worry

SDK - March 31, 2012, 9:40 am

(Mar 25, 2012 04:04 PM)Ralph_Lauren Wrote: [\[CITE\]](#) Has nobody looked at my tutorial :(
Im so sad! did ^^
Nice tut you did, sub from me.

conrad - March 31, 2012, 12:50 pm

(Mar 30, 2012 04:57 PM)Ralph_Lauren Wrote: [\[CITE\]](#) Hmm by default your AWUS036H doesn't come with it's full range capacity for legal reasons.
Some countries have a specific amount of range that they only allow.
Type this in the konsole to increase your adapter to it's full range
root@bt:/# ifconfig wlan0 down
root@bt:/# iw reg set US
root@bt:/# airmon-ng start wlan0
(Then some description about you adapter should show up, then just type the following:)
root@bt:/# iwconfig wlan0
(Now you should see your adapters information, and somewhere in there it should say
"Tx-Power=30 dbm") <-- 30 dbm means success. Mine usually reaches 27 dbm and that's ok. Tell me if I helped you :)
Note: You have to type this in every time you turn on your VMWare
Thank man you're a genius ? worked like a charm on my first target. One thing though on my second try I got 40,000 of data and tried the crack but it failed and said 'next try 5000 IVs' I only had like 20. Is there a way to increase this or should I give up?

Ralph_Lauren - March 31, 2012, 2:40 pm

Some people wait a while (3-5 mins) every time they open a new konsole to type in the next commands in order to fetch more data
For timing reasons I had to hurry up because YouTube only let me put a 10 minute tutorial so I couldn't take my time

seawolve1 - March 31, 2012, 4:29 pm

Great tut....Like to see more of them from you. Keep up the good work!

Ralph_Lauren - March 31, 2012, 9:58 pm

Yes thanks I'm still learning but
enjoy helping the HF community as they have
helped me out so much also

tr!k³³ d!k³³ - April 1, 2012, 4:57 am

Im sorry do people still use wep, these tuts are old now, its manly wpa wpa2, but nice tut.

Ralph_Lauren - April 1, 2012, 1:06 pm

yes people still use wep. In fact in my neighborhood there are twice as much wep than wpa

jdass - April 7, 2012, 6:02 pm

thank you for the tutorial, it worked first time

epsilon972 - April 20, 2012, 7:59 am

Thank you so much as be can it but I can not used the internet in backtrack

Netus90 - May 24, 2012, 11:08 am

???ETUS PETUS GUZANE MARZIANE...ULL

?

(Mar 17, 2012 11:45 AM)david_93 Wrote: [\[CITE\]](#) Hello HF I am releasing my first tutorial that I made on Youtube and I wanted to share it with you guys. It's my first tutorial so please bare with me. This will show you how to crack wep encrypted networks through Backtrack. Please tell me what you think, I am open for any constructive criticism. If you have any questions feel free to PM me :) Thanks!

etuz petus guzane>> uuuull???

(Mar 17, 2012 11:45 AM)david_93 Wrote: [\[CITE\]](#) Hello HF I am releasing my first tutorial that I made on Youtube and I wanted to share it with you guys. It's my first tutorial so please bare with me. This will show you how to crack wep encrypted networks through Backtrack. Please tell me what you think, I am open for any constructive criticism. If you have any questions feel free to PM me :) Thanks!

etus petus guzaneULL???

Biits - November 11, 2012, 1:41 am

Great tutorial!

It'll help starters like us.

rephlex01 - November 14, 2012, 10:51 am

Nice tutorial . keep up the good work

Ram RB - September 11, 2013, 8:41 pm

where is your tutorial, I am not able to see your tutorial??

Habraam - September 22, 2013, 9:33 am

This is a good tutorial... so helpful!!!

sanjay sirvi - October 12, 2013, 8:32 am

great tutorial

well explained

but after i start capturing ivs only beacons are receiving no data is recieved it show 0

plz help me

porcupinelmf - April 24, 2014, 4:28 pm

new to this, so how do I get to view the data? as in the neighbor's PC

j8hax0r - May 13, 2016, 2:04 am

aireplay-ng -9 mon0 not working. how can i fix it ? :(

j8hax0r - May 14, 2016, 12:27 pm

root@Jinthu:~# aireplay-ng -9 wlan0mon

ioctl(SIOCSIWMODE) failed: Device or resource busy

ARP linktype is set to 1 (Ethernet) - expected ARPHRD_IEEE80211, ARPHRD_IEEE80211_FULL or ARPHRD_IEEE80211_PRISM instead. Make sure RFMON is enabled: run 'airmon-ng start wlan0mon <#>'
Sysfs injection support was not found either.

this is my error. anyone help me :(?

j8hax0r - May 17, 2016, 4:56 am

```
root@Jinthu:~# aircrack-ng pre-01.cap -w
/root/Desktop/md5_loweralpha-numeric-symbol32-space#1-7_1.md5sums
Opening pre-01.cap
Read 179163 packets.
```

#	BSSID	ESSID	Encryption
1	30:B5:C2:59:7B:7C	Predator	WPA (0 handshake)

Choosing first network as target.

Opening pre-01.cap
No valid WPA handshakes found..

how can i fix it?

meekoo - May 18, 2016, 9:19 am

where is key code of wireless it is coded?
where I find it ?
:)

pomwtin - May 18, 2016, 9:39 am

(May 18, 2016 09:19 AM)meekoo Wrote: [\[CITE\]](#) where is key code of wireless it is coded?
where I find it ?
:)
Check video at 8:21

For any questions-> wireless help desk:
<https://hackforums.net/showthread.php?tid=4523814>

Hamzah - May 21, 2016, 5:55 am

Thanks man its a great video
keep up the great work

mad.machine - October 2, 2016, 9:29 am

While capturing it creates a sucking situation.what to do?

raykoo expert - April 17, 2017, 8:57 am

good video tnx

ExoticMidnight - June 7, 2019, 9:38 pm

Great TUT looked at it.. APPROVED!!!

enygma - June 22, 2019, 1:07 pm

Thank you very much dear sir!

Black D.180109 - December 7, 2021, 12:10 am

Is that Kali Linux, hacking and stuff specialist

K.worm - March 5, 2024, 4:38 pm

Is this still working at this point?

DramaKing - *March 5, 2024, 4:59 pm*

A 2012 post!? Good grief. Yes, aircrack-ng will still crack WEP passphrases.