

Forum:[Hack Forums](#)

Thread: [Tutorial - WEP cracking with Fern WIFI Cracker - Almost Too Easy!](#)

Spagnum - June 28, 2011, 4:23 am

Warning!

If you want to learn about using Aircrack-ng, Linux, network and so on do not use this tutorial. If you just want to crack a WEP network without learning anything this is the tutorial for you!

Fern Wifi Cracker is a GUI for Aircrack-ng, it makes cracking WEP it so damn simple. I'm on Backtrack 4 here and the only thing you will need download and installing Fern Wifi cracker is to open the terminal and use these two commands: (if you on another distro you might need to install some [packages](#) first)

```
Code wget http://fern-wifi-cracker.googlecode.com/files/Fern-Wifi-Cracker_1.2_all.deb
dpkg -i Fern-Wifi-Cracker_1.2_all.deb
```

To start the program go to:

```
Code /usr/share/applicationsFern_Wifi_Cracker.desktop
```

The first time you open Fern Wifi cracker, you'll need to update it from 1.2 to version 1.5. You will see the text New update is Available

1. Click the Update button

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot1_tilpasset.png[/img]

Wait for the update to be installed. You will see the text Please Restart application

2. Shutdown the application and start it back up again

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot2_tilpasse.png[/img]

You will now see the text Latest update is already installed

3. Click the dropdown list Select interface

4. Select the interface you want to use

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot3_tilpasse.png[/img]

After a minute a popup will open.

5. Click the Ok bottom

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot4_tilpasse.png[/img]

Optional!

The next part might be unnecessary, but it's my personally experience that cracking a network with connected client is much easier then without. Since this is a beginner tutorial I will not go in to why.

6. Doubleclick in any area of the main window

7. A window call Access Point Scan Preferences opens

8. Click the Enable XTerms checkbox

9. Click the Ok bottom

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot5_tilpasse.png[/img]

Let's start sniffing for Accesspoint nearby.

10. Click the Scan bottom

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot6_tilpasse.png[/img]

If you did the part with enabling XTerm - two popups will appear. Since this tutorial will only show WEP cracking you can close the one named FERN (WPA SCAN). Now let's have a look at the window called FERN (WEP SCAN). We need a accesspoint with a client connected to it. At the top half of the screen we see all the accesspoints in the area, and a lot of information about them. At the bottom of the window we see that a client is connected to a Accesspoint with the BSSID 00:13:f7:61:24:DA. If we compare this list in the top of the screen we will see that the name of this Accesspoint is SMC. So now we know that the accesspoint SMC have a client connected.

11. Close the window FERN (WEP SCAN)

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot7_tilpasse.png[/img]

12. Click the WEP button

The window Fern WEP Attack opens.

13. Click the dropdown list at the top of the window

14. Select the access point SMC that we found before

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot9_tilpasse.png[/img]

15. Click the Attack bottom and wait for the magic to happen.

If you did the part with enabling Xterm, two additional windows will open, just leave them be.

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot10_tilpasse.png[/img]

Sit back and wait for the key to the network to appear!

[img]<http://i57.photobucket.com/albums/g207/Spagnum/snapshot13.png>[/img]

'Snorlax - June 28, 2011, 4:32 am

Nice tutorial, very detailed!

Might try it out later ;)

ExobiT - June 28, 2011, 5:59 am

First of all "thanks" for your tutorial. But 1: you forgot the DL link. 2 This app aint working correctly,

just "cracked" my own 40 bit apple wep test network. And it gave me the "key" but the key is far away from the password, and no its not because its showing me it in hex or anything....

Spagnum - June 28, 2011, 7:47 am

(Jun 28, 2011 05:59 AM)ExobiT Wrote: [\[CITE\]](#) 1: you forgot the DL link. 2 This app aint working correctly, just "cracked" my own 40 bit apple wep test network. And it gave me the "key" but the key is far away from the password, and no its not because its showing me it in hex or anything....

1: Danm - I did forget the download link, sorry about that - fixed!

2: It does Work! the key you find is the hash value of the the plain text key salted with the essid of the router. The "app" is using aircrack for the cracking of the key - the result would be the same if you crack WEP keys the "conventional" way with aircrack though the terminal. The key would not be showed in plain text.

Armor-64 - June 28, 2011, 5:16 pm

Hi guys i have a bit of problem!

I am running ubuntu 11.04 and i have installed the app but it's not working..!

It's saying this message...

```
{  
Aircrack-ng and other dependencies need root priviledge to function,Please run application as root.  
}
```

The thing is that i tried to run this as root but nothing.
please help....

Spagnum - June 29, 2011, 1:03 am

(Jun 28, 2011 05:16 PM)Armor-64 Wrote: [\[CITE\]](#) The thing is that i tried to run this as root but nothing.

please help....

what happens when you run the program as root?

CXDBrightSide - June 29, 2011, 1:39 am

Hm, interesting application, but could we get some insight on the WPA function? I'd kinda like to know if this tops Gerix WIFI cracker in any way, which comes stock with BackTrack5 ;) Maybe if it uses JTR or has more options than [insert wordlists/rainbow tables].

Armor-64 - June 29, 2011, 4:01 am

When i am running it as root nothing changes!i have tried from terminal sudo,gksudo,gksu xterm and other things but fail,maybe it's not compatible with ubuntu or something,what system your running maybe i try it there..

Middle - June 29, 2011, 5:01 am

Hey OP nice thread, and its a cool addition, you find nice things i haven't heard of before which i like ^^

However you made a mistake in the title should be 'too easy' not 'to easy'; also yeah it is very easy! But they still need to get on to Linux and have the tool + the adapter, so i see this as a shortcut for those who know what they are doing!

Spagnum - June 29, 2011, 5:08 am

(Jun 29, 2011 04:01 AM)Armor-64 Wrote: [\[CITE\]](#) When i am running it as root nothing changes!i have tried from terminal sudo,gksudo,gksu xterm and other things but fail,maybe it's not compatible

with ubuntu or something, what system you're running maybe i try it there..

What if you log in the graphic interface of Ubuntu with the root user and then run the application?

If you haven't already done i need to enable the root user account with this command in the terminal.

```
sudo passwd root
```

Then choose a password for the root account.

When logging to Ubuntu, press the other account button and use root as username and the password you just entered.

I have tried the application on Backtrack, Ubuntu and Mint, and they all seem to work fine. (I always use the root account when using Linux)

(Jun 29, 2011 01:39 AM)CXDBrightSide Wrote: [\[CITE\]](#) Hm, interesting application, but could we get some insight on the WPA function? I'd kinda like to know if this tops Gerix WIFI cracker in any way, which comes stock with BackTrack5 ;) Maybe if it uses JTR or has more options than [insert wordlists/rainbow tables].

To be honest I haven't play around with the WPA function yet. And either have I in Gerix. I was thinking of making a tutorial of the WPA function later if people like this one.

(Jun 29, 2011 05:01 AM)~Middle Wrote: [\[CITE\]](#) However you made a mistake in the title should be 'too easy' not 'to easy'; also yeah it is very easy! But they still need to get on to Linux and have the tool + the adapter, so i see this as a shortcut for those who know what they are doing!

Damn your right! - can't edit it now. Sorry but english is not my first language. (at least I didn't spell your name wrong in this one ?)

I know newcomers will properly have trouble with general Linux + adapter but still it's hard to explain every little detail and problem they might run in to.

RainbowHat - June 29, 2011, 5:41 am

Will it work on virtual machine? :O

Spagnum - June 29, 2011, 5:51 am

(Jun 29, 2011 05:41 AM)RainbowHat Wrote: [\[CITE\]](#) Will it work on virtual machine? :O

Yes it will. As long as you have a USB wifi adapter.

ignite2030 - June 29, 2011, 10:58 am

well done, thanks for posting.

LiamLC - June 29, 2011, 12:46 pm

I'm new to linux and I'm on BT5. Can you please explain how to install it better? Do you just type in those commands in terminal because that is not working for me. I ended up going to the URL in Firefox and just downloading it but it then when I go to start the program it doesn't work. Please help thanks!

Armor-64 - June 29, 2011, 1:16 pm

Ok it's workin when you are booting as root! thanks man nice post see ya..!

Spagnum - June 29, 2011, 2:07 pm

(Jun 29, 2011 12:46 PM)LiamLC Wrote: [\[CITE\]](#) I'm new to linux and I'm on BT5. Can you please explain how to install it better?

Yup I just download and install with those two commands. Like everything else in Backtrack you need to start the networking service before downloading anything. It can be done in the GUI by

going to service -> Networking or by terminal to entering the command:
/etc/init.d/networking start

(Jun 29, 2011 01:16 PM)Armor-64 Wrote: [\[CITE\]](#) Ok it's workin when you are booting as root!thanks
man nice post see ya..!
Your welcome!

LiamLC - June 29, 2011, 5:43 pm

[IMG]<http://img263.imageshack.us/img263/6726/asfarasiget.png>[/IMG]

That's as far as i get and well... you see the problem. What should I do?

CXDBrightSide - June 30, 2011, 12:12 am

(Jun 29, 2011 05:43 PM)LiamLC Wrote: [\[CITE\]](#)
[IMG]<http://img263.imageshack.us/img263/6726/asfarasiget.png>[/IMG]

That's as far as i get and well... you see the problem. What should I do?
That part confused me as well. I'm pretty sure that's not what he meant to do. Run these and give
me a screenshot with the full windows please:

```
cd /usr/share/applications/ <enter>
ls <enter> Screenshot
```

Now look around for anything mentioning Fern. If you see it,
cd directory found with ls <enter>
ls <enter> Screenshot

Spagnum - June 30, 2011, 12:17 am

I might not have been clear on how to start the application. If you navigate through the GUI to
/usr/share/applications/Fern_Wifi_Cracker.desktop there will be a icon for executing the program
[img]<http://i57.photobucket.com/albums/g207/Spagnum/snapshot14.png>[/img].
if you wanna start the program via the terminal try this command:
python /usr/local/bin/Fern-Wifi-Cracker/execute.py

CXDBrightSide - June 30, 2011, 12:29 am

(Jun 30, 2011 12:17 AM)Spagnum Wrote: [\[CITE\]](#) I might not have been clear on how to start the
application. If you navigate to /usr/share/applications/Fern_Wifi_Cracker.desktop there will be a icon
for executing the program
[img]<http://i57.photobucket.com/albums/g207/Spagnum/snapshot14.png>[/img].
if you wanna start the program via the terminal try this command:
python /usr/local/bin/Fern-Wifi-Cracker/execute.py
applications/Fern_*

Come on man, every time you forget that forward slash you throw Liam off xP
It'd probably be simplest just to click that icon =)

Spagnum - June 30, 2011, 12:35 am

(Jun 30, 2011 12:29 AM)CXDBrightSide Wrote: [\[CITE\]](#) Come on man, every time you forget that
forward slash you throw Liam off xP
It'd probably be simplest just to click that icon =)
aaah fuck now I get it! was the forward slash that I was missing. Sorry about that. Fucking annoying

that I can't edit the original post now...

Stenography - June 30, 2011, 7:14 am

Can someone confirm its really works ? >.<

G-Star Raw - June 30, 2011, 8:07 am

Thanks mate! :) Gunna give this ago later on :P

HackRain - June 30, 2011, 9:35 am

(Jun 30, 2011 07:14 AM)PolarX Wrote: [\[CITE\]](#) Can someone confirm its really works ? >.< confirmed.

=]

like middle said a few threads a go, its shortcut, tool. u still mildly have to know what your doing.

Toaster - June 30, 2011, 2:08 pm

Nice share, thanks mate.Nice share, thanks mate.Nice share, thanks mate.Nice share, thanks mate.Nice share, thanks mate.

G-Star Raw - July 1, 2011, 4:59 am

Ai'nt there a application like this for Windows ?.

Valour - July 1, 2011, 7:20 am

This is really a very good method of cracking into WEP networks. Thanks for posting. I am on windows 7 (Yes it is shit) but I can use it on VMware.... Thanks for posting...

StealthyPriest - July 1, 2011, 9:06 am

Holy crap, I've been looking 4 software this simple for years!!1
Thanks sooo much

Spagnum - July 1, 2011, 10:08 am

(Jul 1, 2011 04:59 AM)G-Star Raw Wrote: [\[CITE\]](#) Ai'nt there a application like this for Windows ?.
Nope there's no application nearly as simple as this for Windows.

stuky - July 1, 2011, 2:58 pm

I already hacked one of the networks. When i try to hack the same one, or another one it does not work. the ivy stays at 0 or it goes up really slow. Ive waited hours for it to get to XX,XXX Ivy and yet it hasnt cracked it. Also, is there a tutorial for WPA? Thanks

Spagnum - July 5, 2011, 2:08 am

Well if you are not close enough to the AP it will take a long time. As said before I might right a tutorial for the WPA part of this program later on.

No??????? - July 5, 2011, 5:20 pm

This software seems a lot like Gerix or SpoonWEP/WPA but thanks for the share anyway. I will stick to terminal based though. I think this stuff is good to start out with for beginners.

Anonymous1200 - July 5, 2011, 9:42 pm

So, This is like a WEP DDoSer?

fahimjan - July 5, 2011, 10:23 pm

Some one post the fern WIFI Cracker working link !

Spagnum - July 6, 2011, 1:02 am

(Jul 5, 2011 09:42 PM)Anonymous1200 Wrote: [\[CITE\]](#) So, This is like a WEP DDoSer?Nooo... ? - its a GUI fr Aircrack

(Jul 5, 2011 10:23 PM)fahimjan Wrote: [\[CITE\]](#) Some one post the fern WIFI Cracker working link !
The link works fine!

Strongarm - July 6, 2011, 1:32 am

might try this but can i have the Terminal codes for Ubuntu?

Spagnum - July 6, 2011, 1:02 pm

(Jul 6, 2011 01:32 AM)chri872y Wrote: [\[CITE\]](#) might try this but can i have the Terminal codes for Ubuntu?

The code should be that same. But you might need to install the packets:

```
python
python-qt4
macchanger
aircrack-ng
xterm
subversion
```

Just type apt get install -packet- them one by one...

walse - July 7, 2011, 1:32 am

klasse up thanks man for the upload

Vexna - July 7, 2011, 2:44 am

Looks very good, keep it up the good work!

rustyrocks69 - July 7, 2011, 11:02 am

new to most of this, worked with computers most of my life, had a little dabble with linux a few times, and have just been introduced to backtrack5, which i am going to dual boot with jolicloud as it is just a notebook, picked up cheap and am not comfortable installing them onto my main pc, accessing WIFI was my 1st intentions when i got introduced and this has helped me perfectly thank you

K!ller - July 7, 2011, 5:18 pm

it dont detect the lan i am using

Spagnum - July 8, 2011, 12:29 am

(Jul 7, 2011 05:18 PM)K!ller Wrote: [\[CITE\]](#) it dont detect the lan i am using
You mean wlan? and your sure you started the network service?

gambe - July 8, 2011, 3:46 am

Nice tutorial. Will try.
Thanks!

FZ4NZ - July 8, 2011, 7:30 am

Nice GUI

But really, this was super fuck easy to do to being with.

All this does it make it easier for little skids to do it (skids should've been able to before this)

Regardless of that aspect, I'm not here to be a jerk off. It looks great and hey.. if it works. we'll then why not :)

Spagnum - July 12, 2011, 2:36 am

It might be "super fuck easy to do to being with" if your a regulate Linux user, but I think for many Windows user that never been out of a GUI environment it can be very confusing.

Amnesia - July 12, 2011, 4:32 am

thank you for tutto

sorry bad english ?

faiz1120 - July 13, 2011, 12:11 am

I'm trying this and so far it's injecting ivs. Inwonder how long it's suppose to take....about 11k packets?

Spagnum - July 19, 2011, 3:35 am

(Jul 13, 2011 12:11 AM)faiz1120 Wrote: [\[CITE\]](#) I'm trying this and so far it's injecting ivs. Inwonder how long it's suppose to take....about 11k packets?

Hard to say, it all depends on if there is descent signal and if a client is connected and is sending data.

rookie21 - July 23, 2011, 3:47 pm

can i download this on windows 7 which is what i have? or run it through vmware which i also already have? or if not that can i burn a iso image of this to my sandisk flash drive and run it through that? please help i really want to try this

Terj - July 23, 2011, 11:51 pm

Running Ubuntu 11.04, have it installed, everything is fine...I open the program, click update, tells me to restart.

I then restart and the program refuses to open. Am I doing something wrong? I'm the root, it works fine until I update, then it just won't open.

Spagnum - July 24, 2011, 3:55 am

(Jul 23, 2011 03:47 PM)rookie21 Wrote: [\[CITE\]](#) can i download this on windows 7 which is what i have? or run it through vmware which i also already have? or if not that can i burn a iso image of this to my sandisk flash drive and run it through that? please help i really want to try this

Yeah you can do this on VMware, you just need a USB wifi if you doing it this way, card since VMWare can't use the internal.

(Jul 23, 2011 11:51 PM)Terj Wrote: [\[CITE\]](#) Running Ubuntu 11.04, have it installed, everything is fine...I open the program, click update, tells me to restart.

I then restart and the program refuses to open. Am I doing something wrong? I'm the root, it works fine until I update, then it just won't open.

Actually I also tried this ones. Dunno what the problem is. Just install the original package again and try again. Worked for me!

(Jun 28, 2011 04:23 AM)Spagnum Wrote: [\[CITE\]](#) Warning!

If you want to learn about using Aircrack-ng, Linux, network and so on do not use this tutorial. If you just want to crack a WEP network without learning anything this is the tutorial for you!

Fern Wifi Cracker is a GUI for Aircrack-ng, it makes cracking WEP it so damn simple. I'm on Backtrack 4 here and the only thing you will need download and installing Fern Wifi cracker is to open the terminal and use these two commands: (if you on another distro you might need to install some [packages](#) first)

Code `wget http://fern-wifi-cracker.googlecode.com/files/Fern-Wifi-Cracker_1.2_all.deb`

`dpkg -i Fern-Wifi-Cracker_1.2_all.deb`

To start the program go to:

Code `/usr/share/applications/Fern_Wifi_Cracker.desktop`

The first time you open Fern Wifi cracker, you'll need to update it from 1.2 to version 1.5. You will see the text New update is Available

1. Click the Update button

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot1_tilpasset.png[img]

Wait for the update to be installed. You will see the text Please Restart application

2. Shutdown the application and start it back up again

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot2_tilpasse.png[img]

You will now see the text Latest update is already installed

3. Click the dropdown list Select interface

4. Select the interface you want to use

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot3_tilpasse.png[img]

After a minute a popup will open.

5. Click the Ok bottom

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot4_tilpasse.png[img]

Optional!

The next part might be unnecessary, but it's my personally experience that cracking a network with connected client is much easier then without. Since this is a beginner tutorial I will not go in to why.

6. Doubleclick in any area of the main window

7. A window call Access Point Scan Preferences opens

8. Click the Enable XTerms checkbox

9. Click the Ok bottom

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot5_tilpasse.png[img]

Let's start sniffing for Accesspoint nearby.

10. Click the Scan bottom

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot6_tilpasse.png[/img]

If you did the part with enabling XTerm - two popups will appear. Since this tutorial will only show WEP cracking you can close the one named FERN (WPA SCAN). Now let's have a look at the window called FERN (WEP SCAN). We need a accesspoint with a client connected to it. At the top half of the screen we see all the accesspoints in the area, and a lot of information about them. At the bottom of the window we see that a client is connected to a Accesspoint with the BSSID 00:13:f7:61:24:DA. If we compare this list in the top of the screen we will see that the name of this Accesspoint is SMC. So now we know that the accesspoint SMC have a client connected.

11. Close the window FERN (WEP SCAN)

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot7_tilpasse.png[/img]

12. Click the WEP button

The window Fern WEP Attack opens.

13. Click the dropdown list at the top of the window

14. Select the access point SMC that we found before

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot9_tilpasse.png[/img]

15. Click the Attack bottom and wait for the magic to happen.

If you did the part with enabling Xterm, two additional windows will open, just leave them be.

[img]http://i57.photobucket.com/albums/g207/Spagnum/snapshot10_tilpasse.png[/img]

Sit back and wait for the key to the network to appear!

[img]<http://i57.photobucket.com/albums/g207/Spagnum/snapshot13.png>[/img]

Noob question i guess: Would all this work on a Windows Vista?? ?

Spagnum - July 24, 2011, 1:53 pm

(Jul 24, 2011 10:33 AM)xAuditore Wrote: [\[CITE\]](#) Noob question i guess: Would all this work on a Windows Vista?? ?

Please don't quote the full tread... and no it won't, only if your running Linux.

proskid - July 24, 2011, 2:24 pm

nice tutorial keep it up ...

Dayates78 - August 3, 2011, 2:37 pm

Where Is the Download link...

xzramazx - August 3, 2011, 3:57 pm

i dont understand how to open in windows.

May you explain more how to open it?
>.< sori im newbie.

Dejuanxg™ - August 3, 2011, 8:33 pm

(Aug 3, 2011 02:37 PM)Dayates78 Wrote: [\[CITE\]](#) Where Is the Download link...
those lines of code he added are the download link and install lol & xzramazx this is for linux

itznick - August 5, 2011, 6:20 pm

Anyone tested this on backtrack 5 and does it work with it?

Dejuanxg™ - August 5, 2011, 8:35 pm

Yes it works great with 5

itznick - August 6, 2011, 8:44 am

Can anyone tell me where is the terminal? I'm a noob at this...

Edit: Ok I found where is but and downloaded it. After I tried opening the program it says

/usr/share/applicationsFern_Wifi_Cracker.desktop (<---Me trying to execute command to open)

bash: /usr/share/applicationsFern_Wifi_Cracker.desktop: No such file or directory.
(This comes up later)

Edit: Fixed everything and managed to crack 2 wifi networks. You should do a tutorial on WPA
please :D

Spagnum - August 10, 2011, 10:41 am

good you god it working itznick... As I said, I might do a tutorial on the WPA part later...

Sno Fear - August 10, 2011, 12:55 pm

Does anyone maybe know how to hack into wireles secured with WPA2-PSK ?

BTW thanks for this tutorial OP.

TickTockMan - August 10, 2011, 1:02 pm

There are a few tutorials on that in this forum. Try this one for starters.

<https://hackforums.net/showthread.php?tid=687543&highlight=wpa>

Death Tech - August 10, 2011, 2:14 pm

Thanks, it worked on my wep network.

RufioStill - August 11, 2011, 1:04 am

Thanks I really hope this works for me..
I'm getting:

BSSID STATION PWR Rate Lost Packets Probes - All Blank on airodump-ng
(I don't think it's a good thing :(.))

On aireplay-ng i'm getting:

You should also start airodump-ng to capture replies.

Read 9XX packets (got 0 ARP request and 0 ACKs), sent 0 packets...(0 pps)

... Should I let it continue? :/ thanks!

Spagnum - August 12, 2011, 3:34 am

sorry dude, but i think your to far away from the AP...

iNk Jr. - August 15, 2011, 12:54 am

Very Nice tutorial. Should help alot of Memebbers ! Trying this now ;)

Chocothunda - August 15, 2011, 12:59 am

Will this work on Windows 7, or is linux required for this?

Error #404 - August 15, 2011, 2:14 am

Nice tool and guide. I'm trying to learn more about Wifi cracking and things of that nature, I would really enjoy if you could make maybe a second topic that tells more about what is really happening behind the interfaces. I want to know more about what is really happening, not just that clicking a button does all these things. Thx (:

jasper388 - August 15, 2011, 7:18 am

can someone help me, backtrack is not recognizing my wifi card

TickTockMan - August 15, 2011, 7:29 am

(Aug 15, 2011 07:18 AM)jasper388 Wrote: [\[CITE\]](#) can someone help me, backtrack is not recognizing my wifi card

More details are needed. What chipset does your wireless adapter have? If you are running it from a virtual machine then you need a usb wireless adapter.

Huredry - August 15, 2011, 7:31 am

This seems very nice. Does it work with Alfa's? Thanks

Spagnum - August 15, 2011, 9:08 am

(Aug 15, 2011 12:59 AM)chocothunda Wrote: [\[CITE\]](#) Will this work on Windows 7, or is linux required for this?

Linux only!

(Aug 15, 2011 02:14 AM)Sythor Wrote: [\[CITE\]](#) Nice tool and guide. I'm trying to learn more about Wifi cracking and things of that nature, I would really enjoy if you could make maybe a second topic that tells more about what is really happening behind the interfaces. I want to know more about what is really happening, not just that clicking a button does all these things. Thx (:

There are lots of other guides in here for that, take a look here:

<https://hackforums.net/showthread.php?tid=162899>

@jasper388 - what TickTockMan said!

(Aug 15, 2011 07:31 AM)Huredry Wrote: [\[CITE\]](#) This seems very nice. Does it work with Alfa's? Thanks

Yup it does - I used a Alfa adapter myself.

Psyclown - August 15, 2011, 11:40 am

Hey OP nice thread and thanks a lot ! U Rock ! I try to learn more 'how to hack' Wifi

sagemsam - August 17, 2011, 5:24 am

Hi,

great tut, even for a beginner like me.

You wrote:

the key you find is the hash value of the the plain text key salted with the essid of the router...

How can I see the key in plain text?

If I connec to the hacked WEP, I have to enter the key in plain text, don`t I?

Spagnum - August 17, 2011, 5:44 am

(Aug 17, 2011 05:24 AM)sagemsam Wrote: [\[CITE\]](#) How can I see the key in plain text?

If I connec to the hacked WEP, I have to enter the key in plain text, don`t I?

You can't! - You can use the hash to log on the network just as well...

bluinblack - August 18, 2011, 5:13 am

When i am running it as root nothing changes!i have tried from terminal sudo,gksudo,gksu xterm and other things but fail,maybe it's not compatible with ubuntu or something,what system your running maybe i try it there.j

t4ng0 - August 18, 2011, 9:57 am

I've got it all set-up and the program updated but still getting the No wireless Interface was found. Yes I'm runnning on virtual machine and I read through post and say gotta have a wireless usb? What is that where can I get something like that so I can run this program on my virtual machine thanks.

I guess I just dont understand why my backtrack can connect via wifi but cant recognize the adapter? Is there anyway to do it without a wireless usb?

slink91 - August 18, 2011, 10:42 am

Thank you for this software it's very great ! I like it !

blueplayer - August 19, 2011, 2:50 am

Seems great! I will try it later at home! ;)

Rezajwz - August 19, 2011, 8:37 am

Nice tutorial thank you for sharing.

/!!

Spagnum - August 20, 2011, 10:17 am

(Aug 18, 2011 05:13 AM)bluinblack Wrote: [\[CITE\]](#) When i am running it as root nothing changes!i have tried from terminal sudo,gksudo,gksu xterm and other things but fail,maybe it's not compatible with ubuntu or something,what system your running maybe i try it there.

Orginal I did it on Backtrack 4, but it does work on Ubuntu as well.

If you navigate through the GUI to /usr/share/applications/Fern_Wifi_Cracker.desktop there will be a icon for executing the program

[img]<http://i57.photobucket.com/albums/g207/Spagnum/snapshot14.png>[/img].

if you wanna start the program via the terminal try this command:
`python /usr/local/bin/Fern-Wifi-Cracker/execute.py`

(Aug 18, 2011 09:57 AM)t4ng0 Wrote: [\[CITE\]](#) I've got it all set-up and the program updated but still getting the No wireless Interface was found. Yes I'm running on virtual machine and I read through post and say gotta have a wireless usb? What is that where can I get something like that so I can run this program on my virtual machine thanks.

I guess I just don't understand why my backtrack can connect via wifi but can't recognize the adapter? Is there anyway to do it without a wireless usb?

You can buy a USB Wifi adapter like Alfa AWUS036H, lots of places online, just google it. The problem with VMware is that it makes the internal wificard act as a Ethernet card on the virtual machine. And the other problem is if you are running Windows as your main OS, the internal wifi adapter will be allocated to Windows.

Retribute - August 20, 2011, 2:23 pm

Hi, I'm in need of some help here.

- 1) When I double click the interface, nothing shows up.
- 2) When I try scanning, it says "Enable monitor mode before scanning"/ "No wireless interface was found".

Any help would be appreciated.

P.S: I opened the application up with Code `sudo python /usr/bin/local/Fern-Wifi-Cracker/execute.py`
P.P.S: I'm dual-booting, not on a virtual machine.

gotestra - August 23, 2011, 11:40 pm

Uh, could I have some help? I'm having two problems:

- 1) I can't seem to configure my wireless device in BT3! Every time I open wireless assistant, it gives the message that "No wireless device has been found. Wireless assistant will now quit."
- 2) The `dpkg -i` command isn't working! When I run it on shell console, it says -bash: dpkg: Command not found
Please help!

Spagnum - August 25, 2011, 11:20 am

(Aug 20, 2011 02:23 PM)RubiksHQ Wrote: [\[CITE\]](#) Hi, I'm in need of some help here.

- 1) When I double click the interface, nothing shows up.
- 2) When I try scanning, it says "Enable monitor mode before scanning"/ "No wireless interface was found".

Any help would be appreciated.

What distro are you using? if you are on backtrack, remember to turn on the networking service before doing anything:

`/etc/init.d/networking start`

(Aug 23, 2011 11:40 PM)gotestra Wrote: [\[CITE\]](#) Uh, could I have some help? I'm having two problems:

- 1) I can't seem to configure my wireless device in BT3! Every time I open wireless assistant, it gives the message that "No wireless device has been found. Wireless assistant will now quit."
- 2) The `dpkg -i` command isn't working! When I run it on shell console, it says -bash: dpkg: Command not found
Please help!

Ones again did you turn on the networking service? - if yes what interfaces do you see if you do a ifconfig in the consol?

llllllllll - August 30, 2011, 1:23 pm

I can confirm this is working on ubuntu. Thanks for the share :)

reda.n - August 30, 2011, 1:44 pm

Yeeah its WOOOrk !! Thanks μYou maaan !!

evilemperor - September 9, 2011, 11:44 pm

Great thread, thanks! I am running a mac and using parallel desktop. I went ahead and installed BT so that it could boot up. Bought an Asus usb wifi dongle and it works great! my question is, do we need to spoof the mac address? I understand it is already done? What if we have already spoofed it?

I found the link didn't work so I just went to the site and downloaded and installed it.

Once you have cracked it, can they tell? Can they tell when you are trying to crack in?

Are there any other ways to get tracked and/or traced?

How about the local ethernet, should we turn that off and use the usb? that's what i did

thanks for the help

Spagnum - September 10, 2011, 4:50 am

(Sep 9, 2011 11:44 PM)evilemperor Wrote: [\[CITE\]](#) my question is, do we need to spoof the mac address? I understand it is already done? What if we have already spoofed it?I believe the program spoofes it itself, so no need to spoof the MAC address manually.

(Sep 9, 2011 11:44 PM)evilemperor Wrote: [\[CITE\]](#) I found the link didn't work so I just went to the site and downloaded and installed it.I don't see a problem with the link?

(Sep 9, 2011 11:44 PM)evilemperor Wrote: [\[CITE\]](#) Once you have cracked it, can they tell? Can they tell when you are trying to crack in?

Are there any other ways to get tracked and/or traced?Some routers keeps logs, and dependent on what kind of attack the program will use some signs of a attack will show up in these logs. - But still it's only the faked MAC address that is being showed. Be aware that if you connect to the router with the cracked password after your done, this will also be logged.

(Sep 9, 2011 11:44 PM)evilemperor Wrote: [\[CITE\]](#) How about the local ethernet, should we turn that off and use the usb? that's what i didNo real reson to turn that one off as I see it...

evilemperor - September 10, 2011, 4:54 am

so if we were to connect to the router after we are done, we should spoof the mac address first?

Spagnum - September 12, 2011, 2:18 pm

If you really want be sure not to be traced - yes you should fake you MAC every time you connect to a cracked AP.

evilemperor - September 12, 2011, 7:56 pm

how do i change my MAC if I am using mac osx? i am using parallels to boot up BT but might want

to access the connection from my macbook

NoOB-| - September 12, 2011, 8:10 pm

wow this is a gr8 tutorial..Thank you for it.

@off-topic... : Can some1 here at HF release a TUT on " How to hack a VPS "

It would be a very kind help...

beastmode16 - September 12, 2011, 9:48 pm

nice share man.. I must try this one.. good you've shared these infos.. More power! Nice job! great!

LORD OF FULL\$ - September 12, 2011, 9:50 pm

I have download the wifi but it did not open on my window 7 it said i should find online for compatible programme for it

Heaven'Perfect - September 12, 2011, 10:12 pm

Do I have to download all those; python

python-qt4

macchanger

aircrack-ng

xterm

subversion

before downloading this program? on Windows 7.

stanedliu - September 12, 2011, 11:29 pm

i found this while i was playing with the file (this was inside it) [data.tar](#)

yep i did this on windows 7

till i found out it doest work with windows 7 ?

[use winrar to open it or 7-zip]

beastmode16 - September 13, 2011, 9:40 pm

dude what is the DL of this app? I wanna try this one.. Thanks in advance!

Spagnum - September 14, 2011, 6:36 am

(Sep 12, 2011 07:56 PM)evilemperor Wrote: [\[CITE\]](#) how do i change my MAC if I am using mac osx?

i am using parallels to boot up BT but might want to access the connection from my macbook

Sorry I'm not a Mac guy, so I can't answer you that...

(Sep 12, 2011 10:12 PM)HeavenPerfect Wrote: [\[CITE\]](#) before downloading this program? on Windows 7.

sorry dude this is Linux only!

(Sep 13, 2011 09:40 PM)beastmode16 Wrote: [\[CITE\]](#) dude what is the DL of this app? I wanna try this one.. Thanks in advance!

It's in the first post: http://fern-wifi-cracker.googlecode.com/files/Fern-Wifi-Cracker_1.2_all.deb

beanheadkid - September 14, 2011, 9:13 am

looks very nice, but hold on, is this illegal?

Spagnum - September 14, 2011, 12:34 pm

(Sep 14, 2011 09:13 AM)beanheadkid Wrote: [\[CITE\]](#) looks very nice, but hold on, is this illegal? The program and method is not illegal in it self, but it's up to you if you use it for illegal cracking some others else's access point.

OriOn - September 16, 2011, 3:08 am

How can i change my mac address in Fern so that i can crack the wep of the AP that has mac filtering. I know the mac add of the connected clients but Fern cannot crack the AP because of filtering. I just want to clone the mac of the associated client so that Fern can automatically attack it but how can i change it on fern.

Spagnum - September 16, 2011, 6:03 am

(Sep 16, 2011 03:08 AM)OriOn Wrote: [\[CITE\]](#) How can i change my mac address in Fern so that i can crack the wep of the AP that has mac filtering. I know the mac add of the connected clients but Fern cannot crack the AP because of filtering. I just want to clone the mac of the associated client so that Fern can automatically attack it but how can i change it on fern.

I don't think you can spoof a specific MAC in Fern, have you tried doing it manually?

jallah_88 - October 19, 2011, 7:30 am

Looking good. 3 networks cracked so far!

wanttocrackwifi - October 23, 2011, 7:53 am

can i use this on Windows? any help i dont know much about Linux so i am confused what to do

Spagnum - October 23, 2011, 12:31 pm

(Oct 23, 2011 07:53 AM)wanttocrackwifi Wrote: [\[CITE\]](#) can i use this on Windows? any help i dont know much about Linux so i am confused what to do

Sorry no, you'll have to learn a few Linux skills for this to work...

Cyber Striker - November 2, 2011, 5:52 am

Hey Spagnum thanks for this wonderful thread but when I click the Scan after selecting the wlan0 I get the two popups but they disappear and I get this in the Konsole

```
sudo python /usr/local/bin/Fern-Wifi-Cracker/execute.py
Unhandled exception in thread started by <bound method mainwindow.scan_wep of
<core.fern.mainwindow object at 0x1da2738>>
Traceback (most recent call last):
  File "/usr/local/bin/Fern-Wifi-Cracker/core/fern.py", line 664, in scan_wep
    wep_access_file = str(reader('/tmp/fern-log/zfern-wep-01.csv')) # WEP access point log file
  File "/usr/local/bin/Fern-Wifi-Cracker/core/functions.py", line 44, in reader
    open_ = open(arg,'r+')
IOError: [Errno 2] No such file or directory: '/tmp/fern-log/zfern-wep-01.csv'
```

and it stays there.. What should I do to fix it? Thank You!

Spagnum - November 2, 2011, 6:39 am

Hi Striker...

hmm... to be honest I never seen that error before. Have you tried reinstalling? Maybe check if you have rwx permissions on the folder or something...

iDuL - November 3, 2011, 3:14 am

This tutorial makes things seem as if it's almost at a click of a button! Good job OP

ViirusMinecraft - August 10, 2012, 9:52 pm

Do you need to download fern in linux or can I download it in my windows 7 and put it on usb? Also I know for a fact the password of the network I want to crack is 10 digits but it says WPA can I still crack it?

Spagnum - August 12, 2012, 9:29 pm

Yes you can download it in windows and then transfer til to Linux if you prefer. No this method is on for WEP protected networks.

anonymous6969 - August 13, 2012, 2:05 pm

hello buddy.i need the download link please i want to try these new method.thanks in advance

QuaRanTinE - August 17, 2012, 12:01 pm

Nice thread, might try it out later =)

SpyFi - August 17, 2012, 4:04 pm

I have used this tool. The programmer who made this also makes GhostPhisher another awesome tool not allowed on HF but worth looking at! Nice tut.

Spagnum - August 18, 2012, 12:33 pm

(Aug 17, 2012 04:04 PM)SpyFi Wrote: [\[CITE\]](#) I have used this tool. The programmer who made this also makes GhostPhisher another awesome tool not allowed on HF but worth looking at! Nice tut. Thanks Spyfi, yeah I have played around with GhostPhiser as well, nice program.

idemo - August 18, 2012, 3:10 pm

I've been using Fern for about 6 months now....initially having a heck of a time getting it installed, but finally working....and then just to discover that it's now included in BT5 R3! Unfortunately they also deleted my favorite program when they did it.. Wep Buster which to me worked much easier and faster than Fern. Fern does have a beautiful interface though and works reasonably well. I like the geographical option. I'd still like to get Wep Buster back...or the old FRHack for BT4 that I have not been able to find a download for anywhere! Not to hijack a thread, but if anyone has FRHack and can upload it to # or somewhere I'd be ever grateful!

Harry8799 - August 18, 2012, 3:50 pm

Nice tool, but it's almost too easy doing it via terminal.