

Forum:[Hack Forums](#)

Thread: [::WiFite:: MASS WEP/WPA CRACKER TUTORIAL::CAN CRACK ALL WEP/WPA](#)

raX0r - October 7, 2011, 12:13 pm

Hi Everyone ?

I'm gonna show you how to crack wep/wpa encrypted networks using WIFITE in backtrack5

::WiFite mass WEP/WPA cracker::

Download link for WiFite at the end of this tutorial

So let's start

Download the Wifite.py

unzip it

command: unzip wifi.py.zip

Spoiler ([Click to View](#))

[img]http://mrblackbeard.my3gb.com/Wifite%20tutz/BT-2011-10-08-00-16-11.jpg[/img]

1 Open a new konsole and Type the path of Wifite

I copied it on my desktop so the command will be

cd Desktop/wifi.py

Spoiler ([Click to View](#))

[img]http://mrblackbeard.my3gb.com/Wifite%20tutz/BT-2011-10-07-22-15-00.jpg[/img]

2 Type the following commands for changing the file permissions to execute or run the file as a program.

chmod +x wifite.py

Spoiler ([Click to View](#))

[img]http://mrblackbeard.my3gb.com/Wifite%20tutz/BT-2011-10-07-22-15-40.jpg[/img]

Hit enter

3 Type ./wifite.py or python wifite.py for starting the program

Spoiler ([Click to View](#))

[img]http://mrblackbeard.my3gb.com/Wifite%20tutz/BT-2011-10-07-22-15-59.jpg[/img]

Hit enter

A box will popup

Spoiler ([Click to View](#))

[img]http://mrblackbeard.my3gb.com/Wifite%20tutz/BT-2011-10-07-22-16-10.jpg[/img]

4 We can crack both wep and wpa networks. I'm taking the wep networks
If you want to crack a specific network "check "the select targets from list option"" otherwise it will start cracking all the available networks
check the "anonymize all attacks" option

Click on the red box for starting the cracking. Once clicked on it a new Konsole will open up

Spoiler ([Click to View](#))

[img]http://mrblackbeard.my3gb.com/Wifite%20tutz/BT-2011-10-07-22-19-37.jpg[/img]

5 Wait till it scans the available networks

6 Press CTRL+C for stopping the scan

Select the network which you want to crack from the list

Spoiler ([Click to View](#))

[img]http://mrblackbeard.my3gb.com/Wifite%20tutz/BT-2011-10-07-22-19-54.jpg[/img]

7 Once you selected the network it will start capturing the packets

Spoiler ([Click to View](#))

[img]http://mrblackbeard.my3gb.com/Wifite%20tutz/BT-2011-10-07-22-29-27.jpg[/img]

Once enough packets have been captured it will start cracking the password

Spoiler ([Click to View](#))

[img]http://mrblackbeard.my3gb.com/Wifite%20tutz/BT-2011-10-07-22-43-12.jpg[/img]

BINGO!!! we got the network key

wpa can also be cracked using this tool ..for that we need a good password list

Hope it was usefull

[Click to download wifite](#)

All comments are welcome, let me know what you think about my post!!
correct my mistakes so i'll never repeat that again ?

[CHECK MY TUTORIAL ON SQLMAP](#)

TickTockMan - October 7, 2011, 12:26 pm

I prefer to go straight to the source when it comes to tools like these, especially free ones. I've used wifite a number of times; its a nice little python script; I still don't understand why the backtrack devs deemed it unworthy of inclusion.

<http://code.google.com/p/wifite/>

raX0r - October 7, 2011, 12:31 pm

(Oct 7, 2011 12:26 PM)TickTockMan Wrote: [\[CITE\]](#) I prefer to go straight to the source when it comes to tools like these, especially free ones.

<http://code.google.com/p/wifite/>

yes bro..you said correctly...I just want to share this for noobs who don't know about it...

tnx for the share ?

Makaveli_360 - October 7, 2011, 1:17 pm

Will this work with any wireless card?

raX0r - October 7, 2011, 1:18 pm

(Oct 7, 2011 01:17 PM)Makaveli_360 Wrote: [\[CITE\]](#) Will this work with any wireless card?
yup work with allmost all wireless card

Makaveli_360 - October 7, 2011, 1:30 pm

What if we want to crack wpa? Do we need anything else? I'm a noob

raX0r - October 7, 2011, 1:44 pm

(Oct 7, 2011 01:30 PM)Makaveli_360 Wrote: [\[CITE\]](#) What if we want to crack wpa? Do we need anything else? I'm a noob
yes you need a good password list and patience..

search on HF you will get good password lists

check the download link on the post u will find info about wpa there...

"Always ready to help"

Greystersting - October 7, 2011, 2:49 pm

Great tutorial! I don't mind clicking adf.ly as long as it's HQ.

theanonymousguy123 - October 7, 2011, 8:41 pm

Thanks dude never tried this, it dont get much easier

raX0r - October 7, 2011, 9:10 pm

(Oct 7, 2011 02:49 PM)Greystersting Wrote: [\[CITE\]](#) Great tutorial! I don't mind clicking adf.ly as long as it's HQ.

? bro..thanx for reading ..

i hope it will help some one.. ?

"correct my mistakes so that i'll never repeat that again"

(Oct 7, 2011 08:41 PM)theanonymousguy123 Wrote: [\[CITE\]](#) Thanks dude never tried this, it dont get much easie

? you are welcome bro....

in this what we want to do is, just select the network and sit simply...the easiest and fastest way....
?

Makaveli_360 - October 7, 2011, 11:42 pm

I get this in mine:

```
wget -O wifite.py http://wifite.googlecode.com/svn/trunk/wifite.py  
wget: invalid option -- 'O'  
Usage: wget [OPTION]... [URL]...
```

Try `wget --help' for more options.

BuckMaster - October 7, 2011, 11:53 pm

great java script for hacking Wep and Wpa.
Cheers!

raX0r - October 8, 2011, 12:19 am

Quote: Makaveli_360' pid='16348393' dateline='1318056172'
I get this in mine:

```
wget -O wifite.py http://wifite.googlecode.com/svn/trunk/wifite.py  
wget: invalid option -- 'O'  
Usage: wget [OPTION]... [URL]...
```

Try `wget --help' for more options.

Sorry about that

Check the new link i've updated it..this time u will get it.... ?

Makaveli_360 - October 8, 2011, 12:29 am

What do you mean copy it in desktop?

raX0r - October 8, 2011, 12:34 am

(Oct 8, 2011 12:29 AM)Makaveli_360 Wrote: [\[CITE\]](#) What do you mean copy it in desktop?
i gotta some probz in my internet connection while typing that post...sorry for that.. check the new reply...

""always ready to help"" ?

(Oct 7, 2011 11:53 PM)BuckMaster Wrote: [\[CITE\]](#) great java script for hacking Wep and Wpa.
Cheers!
It is coded in python ?

Makaveli_360 - October 8, 2011, 2:03 am

Alright I'll try it and report back

raX0r - October 8, 2011, 2:13 am

(Oct 8, 2011 02:03 AM)Makaveli_360 Wrote: [\[CITE\]](#) Alright I'll try it and report back
? Good Luck Bro..

"always ready to help"

Makaveli_360 - October 8, 2011, 7:55 am

I just tried it. Ran into three timeouts. And in the end got 0 cracked. :(Maybe with another network.

theanonymousguy123 - October 8, 2011, 10:26 am

(Oct 8, 2011 07:55 AM)Makaveli_360 Wrote: [\[CITE\]](#) I just tried it. Ran into three timeouts. And in the end got 0 cracked. :(Maybe with another network.

you can change the setting in the gui to not time out, its a checkbox

Makaveli_360 - October 8, 2011, 12:20 pm

(Oct 8, 2011 10:26 AM)theanonymousguy123 Wrote: [\[CITE\]](#) you can change the setting in the gui to not time out, its a checkbox

Alright so when are you supposed to stop the different attacks or whatever?

raX0r - October 8, 2011, 12:27 pm

(Oct 8, 2011 12:20 PM)Makaveli_360 Wrote: [\[CITE\]](#) Alright so when are you supposed to stop the different attacks or whatever?

You have to be within the arp limit of the network which you are cracking...

more closer to the network make data capturing easy ...so it will crack the network key very fast....

Makaveli_360 - October 8, 2011, 12:36 pm

Alright atm it just started cracking. Sorry if I'm being bothersome lol

raX0r - October 8, 2011, 12:49 pm

(Oct 8, 2011 12:36 PM)Makaveli_360 Wrote: [\[CITE\]](#) Alright atm it just started cracking. Sorry if I'm being bothersome lol

he he dont ever feel like that....

"always ready to help"

Makaveli_360 - October 8, 2011, 3:12 pm

How long does it take to crack a 64 bit key? I'm trying to crack mine and its been over 2 hours.

What are you supposed to do if you set it to endless? Like when are you supposed to stop each attack? After stopping all of them nothing happened.

FZ4NZ - October 8, 2011, 9:52 pm

Nice bit of automation there, nice to see some scripts that are useful.. I don't really need it but it would speed things up I suppose

(Oct 8, 2011 03:12 PM)Makaveli_360 Wrote: [\[CITE\]](#) How long does it take to crack a 64 bit key? I'm trying to crack mine and its been over 2 hours.

What are you supposed to do if you set it to endless? Like when are you supposed to stop each attack? After stopping all of them nothing happened.

Your going way to long... Your talking about a WEP 64 bit key right?

Do you have packet injection? About 50-70K IVs should crack it... actually with a 64 bit key even 30K or as little as 11K could crack the key depending on complexity... If you don't have injection it'll take quite a while..

If you don't have any clients on the network try to forge a packet using packetforge and use aireplay to inject it back out into the network... or assuming your having trouble with fake authentication with the router.. attack a client and get the key by collecting IVs generated by the client/station

Makaveli_360 - October 8, 2011, 10:27 pm

I think I have injection cause it goes at about 250-300 IVs/sec. I'll try it again with a 10 minute time out like it originally says. There's three clients on the network excluding the computer which was turned off.

yindia - October 9, 2011, 6:52 am

what if the password is some indian name which is not in the password list.. is there any way to brute force it here ?

TickTockMan - October 9, 2011, 7:25 am

(Oct 9, 2011 06:52 AM)yindia Wrote: [\[CITE\]](#) what if the password is some indian name which is not in the password list.. is there any way to brute force it here ?

A dictionary attack requires that the passphrase be in the list, of course. See if you can obtain a list of command indian names.

bestcarbmw - October 9, 2011, 11:45 am

i will try if it is working thank you :)

kof123 - October 9, 2011, 12:41 pm

(Oct 8, 2011 10:27 PM)Makaveli_360 Wrote: [\[CITE\]](#) I think I have injection cause it goes at about 250-300 IVs/sec. I'll try it again with a 10 minute time out like it originally says. There's three clients on the network excluding the computer which was turned off.

i think im having the same issue, treid it a few times dont know whats the problem

raX0r - October 9, 2011, 8:51 pm

(Oct 9, 2011 12:41 PM)kof123 Wrote: [\[CITE\]](#) i think im having the same issue, treid it a few times dont know whats the problem

The network which you are cracking should have good data traffic.... then only it can capture the data packets....It will take hardly 5-8 mints for cracking a network with high data transfer rate..

try to be close to the wireless network so that u can crack it ... ?

lucaswalterwyland - October 9, 2011, 11:27 pm

thanks for this man nice job:) way to go in detail too

Makaveli_360 - October 10, 2011, 9:45 am

Doesn't work at all for me. I selected the arp replay attack only on a 30 minute time out. It said it started cracking at +9000 and I left the computer on all night. Had already retrieved 11,000,000 IVs with no progress really. Thanks though.

LaZaRynth - October 10, 2011, 10:23 am

raxor Great find! i'm using this as we speak, makes cracking WEP alot less taxing then having to jump around playing with commands over and over again, very cool little program!

thanks for the link! much appreshiated!

BuckMaster - October 10, 2011, 10:42 am

anyone can test the trunk version revision 82 too.

here is the dl link:

<http://code.google.com/p/wifite/source/browse/trunk/wifite.py>

Cheers!

theanonymousguy123 - October 10, 2011, 5:46 pm

(Oct 10, 2011 10:42 AM)BuckMaster Wrote: [\[CITE\]](#) anyone can test the trunk version revision 82 too. here is the dl link:

<http://code.google.com/p/wifite/source/browse/trunk/wifite.py>

Cheers!

Hey broseph, how do you compile the trunk code(noob question)? I tried pasting it into a shell and nothing happened; maybe its over my current rookie linux abilities...

yindia - October 16, 2011, 6:13 am

save the .py file and type ./filename from the terminal.

One qn though, it says - key cracked and gives a big key and also the ascii form. which like in the screen posted initially is a set of consecutive numbers like 0987654321 .. how do we proceed from here..

raX0r - October 16, 2011, 6:21 am

(Oct 16, 2011 06:13 AM)yindia Wrote: [\[CITE\]](#) save the .py file and type ./filename from the terminal.

One qn though, it says - key cracked and gives a big key and also the ascii form. which like in the screen posted initially is a set of consecutive numbers like 0987654321 .. how do we proceed from here..

If it is wep then that is the network key..once logon to the network with that numbers and check it...!

docker - October 16, 2011, 7:08 pm

hello, can i use this software for windows OS??

TickTockMan - October 16, 2011, 7:11 pm

(Oct 16, 2011 07:08 PM)docker Wrote: [\[CITE\]](#) hello, can i use this software for windows OS??

If you had visited the wifite site, which I gave the link to previously, you would have seen the following:

designed for Backtrack4 distribution of Ubuntu; works great with BlackBuntu! Linux only; no windows or osx support.

anarkyst - November 20, 2011, 10:55 pm

I'll holler back about success/failure once I can collect enough data packets.

Since the interface is cooler (with pyrit), you might update the post to mention it.

Thanks.

?A?O - November 21, 2011, 11:29 am

(Oct 7, 2011 12:26 PM)TickTockMan Wrote: [\[CITE\]](#) I prefer to go straight to the source when it comes to tools like these, especially free ones. I've used wifite a number of times; its a nice little python script; I still don't understand why the backtrack devs deemed it unworthy of inclusion.

<http://code.google.com/p/wifite/>

Thanks for that. I like learning something new from just text instead of a GUI.

You'll never learn anything by always using different GUIs.

raX0r - November 21, 2011, 6:18 pm

(Nov 21, 2011 12:29 PM)?z??o Wrote: [\[CITE\]](#) Thanks for that. I like learning something new from just text instead of a GUI.

You'll never learn anything by always using different GUIs.

Mate....agreeing with you...

btwn I also learned it from that link only...!!!?

A++++ - December 12, 2011, 4:16 am

That was a great tutorial and so simple. Thanks for sharing.

Rosmo - December 12, 2011, 1:09 pm

Ive been for years trying to crack wifi as u know nowadays all are using WPA but i will try, Im using Netgear WG 111 v 3, is it working for WPA crack. Thanks for your kindness

RoyalShady - December 12, 2011, 2:39 pm

Thank You for this I will try it soon !

raX0r - December 14, 2011, 8:02 pm

Glad that it helped someone.

Thanks for the feedback's. ?

ACM1PT - December 15, 2011, 8:35 am

thx for upload very nice

i will try it out

nightwolf2883 - December 15, 2011, 3:36 pm

thank you for sharing this with us =)

TonyS - December 15, 2011, 4:50 pm

does backtrack5 on work wit usb cards ?

HackRain - December 15, 2011, 5:31 pm

Yeah.. Great. Just what I like to see..

Another tool dedicated to fucking skid's!

Iv spent nearly 1 year in wireless section learning about injection techniques and Working on learning how to manipulate all wireless security..

And you just come along and post a tool that literally said something like " haxx0r but0n" Auto hack shit..

I really don't support this, my hard experience has been stuffed into one shut little GUI auto haxor. Why even post this, your giving these kids a reason to say I I'm a. L337 haxor.. No learning no intelligence no hardworking.. Just auto haxxor.

Seeing hack.exe shits me off. The chances are if you even use this tool, it probably because your lazy and have no intention tonput hard work in, but simply want results.

Sorry, but this software isn't supported by the bt team and I highly recommend for the creditability of this sub forum that you guys look at it the same as myself.

If this section becomes filled with hack.exe it looses the point of hacking.

I'd think for anyone who enjoys exploiting and manipulating to discourage tools like this.

As someone has automated our hard work.

(Dec 15, 2011 05:50 PM)TonyS Wrote: [\[CITE\]](#) does backtrack5 on work wit usb cards ?Prime example.. No?

This is going to be the hackers of the future.

raX0r - December 15, 2011, 7:38 pm

(Dec 15, 2011 06:31 PM)PandaMonix Wrote: [\[CITE\]](#) Yeah.. Great. Just what I like to see..

Another tool dedicated to fucking skid's!

Iv spent nearly 1 year in wireless section learning about injection techniques and Working on learning how to manipulate all wireless security..

And you just come along and post a tool that literally said something like " haxx0r but0n" Auto hack shit..

I really don't support this, my hard experience has been stuffed into one shut little GUI auto haxor. Why even post this, your giving these kids a reason to say I I'm a. L337 haxor.. No learning no intelligence no hardworking.. Just auto haxxor.

Seeing hack.exe shits me off. The chances are if you even use this tool, it probably because your lazy and have no intention tonput hard work in, but simply want results.

Sorry, but this software isn't supported by the bt team and I highly recommend for the creditability of this sub forum that you guys look at it the same as myself.

If this section becomes filled with hack.exe it looses the point of hacking.

I'd think for anyone who enjoys exploiting and manipulating to discourage tools like this.

As someone has automated our hard work.

Prime example.. No?

This is going to be the hackers of the future.

Thanks for your feedback sir.

As you know that hardworking guys are very rare to find here.All are seeking help of tools to do their work(including me),It never make anyone a l33t haxor.Hardworking is the path towards l33t.

I just shared my little knowledge about the tool to others(only good intention),thought it will help at least someone here.

Sir i'm really sorry if it disturbs you.

HackRain - December 16, 2011, 7:12 pm

No no, that's fine. I appreciate your sharing of knowledge. It's great too see.

I just was sharing my opinion of this particular topic.

raX0r - December 16, 2011, 8:52 pm

Sir thanks for your gift.

I can't PM you because I'm not in your buddylist ?

Danial1369 - December 17, 2011, 7:08 am

thanks,but this software is not good.

vinerpiz - December 17, 2011, 10:33 am

does this works? someone tested?

thanks in advance

rowebil - December 18, 2011, 6:26 pm

(Dec 16, 2011 08:12 PM)PandaMonix Wrote: [\[CITE\]](#) No no, that's fine. I appreciate your sharing of knowledge. It's great too see.

I just was sharing my opinion of this particular topic.

Damn. You really did share your opinion.

Relax haha.

I've been doing Wireless hacking for a while as well, but I don't think WiFite is a bad program. Doesn't look too bad.

PickingUpShit - December 19, 2011, 7:33 pm

The fake authentication doesn't work on any of my wifi connections. They're all within range and has good connection. What am I suppose to do know? For the WPA it doesn't get any handshakes..

belyan789 - January 17, 2012, 3:42 am

i will try this procedure thanks man im newbies

Mauri - January 17, 2012, 11:17 am

here you can find a video tutorial for that tool:

<http://maurisdump.blogspot.com/2011/12/fully-automated-mass-wpa-wep-hacker.html>

Fishy - January 18, 2012, 10:29 am

Great tutorial!!! This was an simple and awesome tutorial for this :) Thanks.

-Oh- - January 18, 2012, 1:41 pm

thanks dude. keepup the good work. Lol fast typed comment i am a N00B.

piffkush - January 18, 2012, 8:28 pm

(Dec 15, 2011 06:31 PM)PandaMonix Wrote: [\[CITE\]](#) Yeah.. Great. Just what I like to see..

Another tool dedicated to fucking skid's!

Iv spent nearly 1 year in wireless section learning about injection techniques and Working on learning how to manipulate all wireless security..

And you just come along and post a tool that literally said something like " haxx0r but0n" Auto hack shit..

I really don't support this, my hard experience has been stuffed into one shut little GUI auto haxor. Why even post this, your giving these kids a reason to say I I'm a. L337 haxor.. No learning no intelligence no hardworking.. Just auto haxxor.

Seeing hack.exe shifts me off. The chances are if you even use this tool, it probably because your lazy and have no intention tonput hard work in, but simply want results.

Sorry, but this software isn't supported by the bt team and I highly recommend for the creditability of this sub forum that you guys look at it the same as myself.

If this section becomes filled with hack.exe it loses the point of hacking.

I'd think for anyone who enjoys exploiting and manipulating to discourage tools like this.

As someone has automated our hard work.

Prime example.. No?

This is going to be the hackers of the future.

well things are getting easier. I make music videos with special effects and the other day my lil brother had a iphone app that adds a car exploding in the background.

learn to embrace technology. dont be mad because its getting easier

V3R7!90 - January 24, 2012, 12:55 pm

Its captures so sloww 0.0 4 min 1 ivs :[0/sec

and the target is 30dB how come it dosnt work? and why the target has CLIENT next to it?

Un-Named - January 24, 2012, 2:42 pm

For WPA it took me 10 hours.

WEP Took me 15 minutes.

Just a little tip to those.

There's a big difference between WPA and WEP.

Anonymiss - January 24, 2012, 9:17 pm

i think the links broken now, or is it just me? i go to download WiFite and it says im not able to. Is it just me?

Mauri - January 24, 2012, 9:41 pm

checkout my signature for another wifite tutorial. i know the author well, so its no suprise that my tutorial video is on his frontpage :)

Joshtheterrible1 - January 24, 2012, 9:47 pm

the website says

All sharing functionality on FileSonic is now disabled. Our service can only be used to upload and retrieve files that you have uploaded personally.

If this file belongs to you, please login to download it directly from your file manager.

SpicyHacker - January 24, 2012, 10:27 pm

(Jan 24, 2012 10:47 PM)Joshtheterrible1 Wrote: [CITE](#) the website says

All sharing functionality on FileSonic is now disabled. Our service can only be used to upload and retrieve files that you have uploaded personally.

If this file belongs to you, please login to download it directly from your file manager.

yeah i get the same ...so its not just you ?

Anonymiss - January 24, 2012, 11:17 pm

Well that sucks, ima go look at the other tut then

Nieeli - January 25, 2012, 12:40 am

Broken link.. I want this so badly lol, im with my phone's connection online n theres a wep near :O

V3R7!90 - January 25, 2012, 5:20 am

Guys! use the link from TikTokMan (2nd post)

murdokZor - January 25, 2012, 8:24 am

wow, i ll check it out!, :) thanks!

Tinno4sure - January 25, 2012, 10:17 am

Can you tell me where i can download it ??
also work with windown xp or only LINUX ?

V3R7!90 - January 25, 2012, 11:00 am

(Jan 25, 2012 11:17 AM)Tinno4sure Wrote: [\[CITE\]](#) Can you tell me where i can download it ??
also work with windown xp or only LINUX ?

<http://code.google.com/p/wifite/>

Only linux,(ubuntu, bt)

I cracked one with it already im busy with another
one atm but somehow it takes very long this time
i have 1,2 mil ivs already lol

Commander 11:11 - August 14, 2013, 6:34 am

OP can you update the pictures in tutorial! They don't work...And I can't download the wifite trough
the link you provided!!

Please can you post new download link?? :/

I really need this!!

Thank you in advance!!

dadonnon - August 14, 2013, 10:48 am

I use wifite.py back in the day, and it is very depandable

Commander 11:11 - August 14, 2013, 10:52 am

(Aug 14, 2013 10:48 AM)dadonnon Wrote: [\[CITE\]](#) I use wifite.py back in the day, and it is very
depandable

Do you have any good tutorial on wifite.py???

antonislina - November 9, 2013, 3:22 am

the link dont work help it saying doesnt excist ,,thanks