

Forum:[Hack Forums](#)

Thread: [\[TUT\] Crack Windows password using Ophcrack \[TUT\]](#)

Combobreaker - October 17, 2010, 6:13 am

Hi!

This will be some amount of text - but if you want the administrators password or any user on the Windows System, this is the guide for you.

I haven't found any guide that explains very detailed on how to get this to work, so I am going to go through some basic steps and tell you how to do!

First of all, here's some parts you need to think about:

- Physical access (You need to sit at the computer, as in school etc)
- You need a CD/DVD and a ROM-reader (That can read the CD or DVD) (The reader often is in the computer... ?)
- It will take some time, so if you got ten seconds on you to go, this may not be the thing for you. This procedure could take up to 10 minutes (depending on the password, and how many passwords you're cracking)

Alright - with that done, let's get down to the fun part! ?

1. Download Ophcrack <http://ophcrack.sourceforge.net/> (Select the LiveCD installation)
2. When that is done, download a .iso burner - use any kind that will fit your needs, for example Nero Burner. (Personally I use CDBurnerXP, works really good and is easy)
3. Put the .iso file you downloaded (The ophcrack) on the CD or DVD. (I use DVD since it has more space and is more reliable in my opinion)

NEXT STEPS DO NOT REQUIRE THE SAME COMPUTER AS THE ONE YOU DOWNLOADED OPHCRACK ON!?

4. Start up the computer you are going to crack passwords on.
5. Put in the CD or DVD in the tray, and close.
6. Shut the computer down, and then start it again.
7. Select that you want to boot from the ROM, often that option is at F2, F6 or ESC, depending on your computer. (This allows you to boot a new "system" based on the information that is on your DVD)
8. After a while, you will see an interface based on some people on the left side, with OPHCrack logo and stuff, and then text on the right.
Highlight the option at the top, that says something close to OPHCracked Graphic Mode (It should be default highlighted) and press enter.
9. Now this part could take some while, maybe up to 2-3 minutes depending on your machine.
10. You get into a platform very similar to the BackTrack 4 one (Where you have the menu and all that, not just the console), and then it will start up a program by itself. The program is (start the drums) OPHCRACK!

Alright. Now we have:

Booted the CD/DVD, we are NOT logged in at Windows platform. If you are, or anything else isn't the way I have explained, repeat the other steps.

The system has also started the OPHCRACK and we should see a white interface (Very niet)
We should see the users of the computer inside the Ophcrack box.

11. Alright, we see the full list of users on the computer in the left column, delete all the other than the ones you want to crack password on. (You may need to press the red X (stop) at the top if the Cracker is already running by default settings.)

12. Press Crack.

13. There is some things that need to be loaded, such as the Brute-Forcer, and the RAM-memory shall be up to 100% - then the "Process" should start.

14. The passwords starts to come together as the Process is going on.

And after some time you get the whole password, next to the username.

Time for cracking:

Three users:

User1, password=979aolkx98

User2, password=skit976ner82dig

User3, password=89skolp7cra

To crack these three users took me about 4-5 minutes (Exclusive the startup and boot the DVD etc)

This is a very reliable method that I have used in school to get the Administrators password when the computers wasn't watched by someone.

Alright - that is just the basics to get the password for administrator on Windows.

OTHER:

I know I have been using plain text and no hilarious pictures etc - but this is just what you need, if you follow this guide I'm sure you will get what you want.

'Til next time HF!

(Correct me with some information if you like)

Ludde420

Gibson - October 17, 2010, 7:14 am

Nice tut!

Must have taken a while to make this

But one thing, if i download the 'live cd' will it burn it straight to a CD if i have one inserted?

Combobreaker - October 17, 2010, 7:39 am

Download the Live CD version - and then just put it on the desktop.

Then find a disc that can take 415 mb and use a program to burn it to the disk.

I use the program CDBurnerXP - works like a charm all the time I put something on the CD!

(The file you should burn over to the disk is "ophcrack-xp-livecd-2.3.1" and it's an ISO-file)

SIM-353284 - October 17, 2010, 7:40 am

rated thread ?

nice tut.

Ohya - October 17, 2010, 7:53 am

Nice thread,
Thanks for the Share.
Bookmarked and will try it out later.

vienquay - *October 17, 2010, 9:06 pm*

Nice tutorial, very well written and easy to understand for beginners. A must-bookmark for someone starting out in the hacking business.

-Mr Mesmer - *October 17, 2010, 9:12 pm*

(Oct 17, 2010 07:14 AM)Gibson Wrote: [CITE](#) But one thing, if i download the 'live cd' will it burn it straight to a CD if i have one inserted?
I was actually wondering the same thing.

Northandos - *November 9, 2010, 8:29 pm*

I just ran This On My Vista Computer From Boot, It Found Out the first Simple Password for 1 user : training, But It Failed to find the password for the other user which was rinlar756 Why Would this be?

zer0day - *November 9, 2010, 8:49 pm*

Nice Tut but you should have included how to put Ophcrack on a USB also, way easier than burning an image and you dont waste a CD. Check the sig for tools to use with the Tut. Thanks for sharing.

GuJJu - *November 9, 2010, 8:50 pm*

Nice tutorial and thanks for the Share. Will try out later when i have plenty of time. ?

Cyber`SoLdier - *December 22, 2010, 11:22 am*

Nice TUT just two questions - Will this work on Windows 7? and Can I use the CD more times, or just once?

I need to get administrator access to a Computer running Windows 7 and who knows when I'll need the Ophcrack again ?

Thanks for share totally trying this !

-kREEDz