

Forum:[Hack Forums](#)

Thread: [How to hack/recover a windows password in <20 minutes \[TUT\]](#)

?ICE? - March 25, 2013, 9:42 pm

Hi everyone, wanted to create an easy tutorial on how to hack a Windows XP/Vista/7/[Not sure about 8] password in about 20 minutes or less. Anyways, lets get started.

WHAT YOU WILL NEED:

---USB 4 GB or more

---Backtrack 5 R3 [FREE]

<http://www.backtrack-linux.org/downloads/>

---Unetbootin: <http://goo.gl/N0syu>

—

---STEP 1: Ok, now that we have all that, take your usb, and plug it into your own computer.

--STEP 2: Open up Unetbootin (will require admin privileges) and select Disk image, ISO, and then browse to the ISO you downloaded from one of the above links. Select USB drive, or hard disk if you are using one, and select the proper drive. Then click OK.

--STEP 3: When Unetbootin finishes, it will ask you to reboot. Just close out of that, and then eject the usb.

--STEP 4: Plug the USB into the computer you are hacking(doesn't matter if the system is on or off) and then restart your computer, or boot it up if already off. Depending what model you have, when booting there should be an option such as (for hp) "Press ESC for more options". Depending on what to press, do this, and then do the following:

If there is a label "boot options", press the desired key to get there, and chose your usb.

If there is not a label "boot options", and just a bluish old fashioned screen, navigate to boot options (sorry, don;t remember the exact path) and move your usb to the first boot option.

--STEP 5: If you have successfully booted, then you should be presented by a screen with options such as

"Default"

"Default Text Mode"

etc.

Ok, just press enter, and you should see a lot of code flying down the screen.

When the code stops, and there is a red text containing Code root@bt type in the following commands.

Code mkdir /mnt/win

mount -t ntfs /dev/sda1 /mnt/win

cd /mnt/win/Windows/System32 Not Command--Just if you are presented with an error, such as the

directory doesn't exist, then type in the following: `mount -t ntfs /dev/sda2 /mnt/win7` If there was no error, then just continue on and type in the code below.

Code startx

(you should be presented by a screen with a dragon and "backtrack 5" background)

---STEP 6: In the top right click on system, then home folder. Almost like in windows explorer, how in the left there is documents, music, pictures....just click on 'File system', and you should be presented with different folders. Go into `mnt-->win` (if you had an error before in step 5, go to `win7`)-->Windows-->System32

---STEP 7: After the System32 folder loads up *might take from 10 seconds to a minute navigate to a file with the name of 'sethc.exe'. This is the sticky keys file. If you use sticky keys, or don't want to get rid of them, put this file on a usb to restore to your computer later, but either way, delete the file from the folder.

---STEP 8: Find the file named 'cmd.exe' and rename it to 'sethc.exe'.

---STEP 9: Take out your usb and then reboot your computer, windows should load up if you took out the usb with backtrack on it.

---STEP 10: when you are at the windows login screen, hit the shift key 5 times in a row until a command dialouge pops up. You now have administrator rights in command prompt

---STEP 11: Enter this code in the command promp-

Code net user

This should display the current users on the computer.

---STEP 12: Then enter this code with Username being replaced by the username (ex: John) you must recover the password from-

Code net user Username *

---STEP 13: You should be presented by "type a new password for the user:"

---STEP 14: Enter the password you want, and you have hacked the account ! After gaining access to the computer, be sure to go to 'Windows-->System32' and rename 'sethc.exe' to 'cmd.exe'. If you saved the original sethc.exe file, drag it into the folder, and your good to go. Otherwise the person's computer's command prompt will be sethc.exe instead of cmd.exe

OTHER COMMANDS:

Give admin acces to user:

Code net localgroup administrators USERNAME /add

Take admin rights away from user:

Code net localgroup administrators USERNAME /delete

PedroDJ - March 27, 2013, 4:53 am

(Mar 27, 2013 04:50 AM)parislvr wrote: [\[CITE\]](#) Penetrate Computer Via Facebook Only

Vedio - Download Link >>> <http://ge.tt/4ZJhZHc/v/0>

New Program By Anonymous

there is a simpler way than this

Hack Computer With Anonymous V 1.0.2



Download Link : <http://ge.tt/122qY4c/v/0>

.EXE

Download Link :

<http://utox.webs.com/Hack%20Computer%20With%20Anonymous%20V%201.0.5.rar>

.Rar

The best Program In the World

<http://anonymous-hacking.webs.com/>

Infected link: post reported.

This is the same stupid user of yesterday, that's spreading virus on HF.

Please ban.

(Mar 27, 2013 04:50 AM)parislvr wrote: [\[CITE\]](#) Penetrate Computer Via Facebook Only

Vedio - Download Link >>> <http://ge.tt/4ZJhZHc/v/0>

New Program By Anonymous

there is a simpler way than this

Hack Computer With Anonymous V 1.0.2



Download Link : <http://ge.tt/122qY4c/v/0>

.EXE

Download Link :

<http://utox.webs.com/Hack%20Computer%20With%20Anonymous%20V%201.0.5.rar>

.Rar

The best Program In the World

<http://anonymous-hacking.webs.com/>

Infected link: post reported.

This is the same stupid user of yesterday, that's spreading virus on HF.

Please ban.

?ICE? - March 27, 2013, 1:41 pm

PedroDJ, what does that user have to do with this thread?

f00bar - March 27, 2013, 1:44 pm

you do know there is a simple program to put on a usb boot it up and it will bypass the password
lmao

?ICE? - March 27, 2013, 5:21 pm

Really, lol? What's it called? Would really like to check it out.

LittleBobbyTables - March 27, 2013, 6:51 pm

Konboot, the official link is <http://www.piotrbania.com/all/kon-boot/>