

Forum:[Hack Forums](#)

Thread: [Hack Windows Password in Less than one Minute without admin privilege](#)

Vaxorr - September 8, 2014, 10:02 am

Well i found this method, its not saturated and yeah i saw this method work actually.

Here is The Tutorial :

Firstly Download Hiren's Boot from this direct link from official website :

<http://www.hirensbootcd.org/files/Hirens.BootCD.15.2.zip>

and you will have to burn it to a CD or a USB.

Boot your computer with Hiren's BootCD and follow the steps below for resetting your password:

1. Enter "Offline NT/2000/XP/Vista/7 Password Changer"

With Up & Down keys select Offline 'NT/2000/XP/Vista/7 Password Changer' and press Enter.

2. Wait for "Offline NT Password & Registry Editor" to Load

On the screen below, you'll see is several lines of text that quickly run down the screen. You don't need to do anything here. Wait for "Offline NT Password & Registry Editor" to load.

Select "NT/2000/XP/Vista/7 Password Changer" :

[img]http://www.hirensbootcd.org/images/resetting_win_password/choose_password_changer.png[img]

2. Linux files are loading...

[img]http://www.hirensbootcd.org/images/resetting_win_password/linux_files_are_loading.jpg[img]

3. Choose the Correct Hard Drive Partition

This step in the Offline NT Password & Registry Editor process is to select the partition that contains the Windows installation that you want to delete a password from.

Many computers have a single operating system installed on a single partition on a single hard drive, making this a very easy choice.

If that's the case for you, just press ENTER to accept the default partition. Otherwise, type the number corresponding to the correct partition from the Candidate Windows partitions found list and then press ENTER.

4. Confirm the Windows Registry Path

Offline NT Password & Registry Editor now needs to know the exact location of the Windows Registry. Except in the rarest of occasions, the default location will be the correct one.

Just Press ENTER to accept the default Windows Registry path without writing anything else.

Choose the Correct Hard Drive Partition

[img]http://www.hirensbootcd.org/images/resetting_win_password/choose_hard_drive_partition.jpg[/img]

4. Confirm the Windows Registry Path

[img]http://www.hirensbootcd.org/images/resetting_win_password/confirm_the_windows_registry_path.jpg[/img]

5. Choose the Password Reset Option

Offline NT Password & Registry Editor is now asking which part of the registry it should load.
Press ENTER to accept the default choice of Password reset.

6. Choose the Edit User Data and Passwords Option

Now that the registry is loaded and available to the program, Offline NT Password & Registry Editor needs to know exactly what you want to do.
Press ENTER to accept the default choice of Edit user data and passwords.
This will load the necessary options for the actual password reset.

Choose the Password Reset Option

[img]http://www.hirensbootcd.org/images/resetting_win_password/choose_the_password_reset_option.jpg[/img]

Choose the Edit User Data and Passwords Option

[img]http://www.hirensbootcd.org/images/resetting_win_password/choose_edit_user_data_and_passwords_option.jpg[/img]

7. Enter the Username to Edit

Offline NT Password & Registry Editor now needs to know which user's password you'd like to delete (erase, clear, blank, remove, call it what you like).
A default user is listed between the brackets at the prompt. In the above example, you can see that it's the Administrator user.
If the default user is the user you'd like to remove the password from, simply press ENTER.
Otherwise, enter the username and then press ENTER.

8. Type 1 to Clear (blank) user password and then press ENTER

At the bottom of the screen you'll see the User Edit Menu with several options to choose from.
Type 1 for Clear (blank) user password and then press ENTER.

Enter the Username to Edit

[img]http://www.hirensbootcd.org/images/resetting_win_password/enter_the_username_to_edit.jpg[/img]

Type 1 to Clear (blank) user password and then press ENTER

[img]http://www.hirensbootcd.org/images/resetting_win_password/type_1_to_clear_password.jpg[/img]

9. Type ! to quit the User Edit Tool

Assuming there weren't any problems, you should see a Password cleared! message after entering 1 in the previous step.

Type ! to quit editing user and then press ENTER.

10. Type q to Quit Offline NT Password & Registry Editor

Enter q and then press ENTER to quit the Offline NT Password & Registry Editor registry editing tool.

Important: You're still not done! You need to confirm your password reset change in the next step before it will take effect.

Type ! to quit the User Edit Tool

[img]http://www.hirensbootcd.org/images/resetting_win_password/quit_the_user_edit_tool.jpg[/img]

10. Type q to Quit Offline NT Password & Registry Editor

[img]http://www.hirensbootcd.org/images/resetting_win_password/confirm_that_youare_finished.jpg[/img]

well and remove the CD and restart the computer and its all fine and the password is removed!

Video :

[Video: <http://vimeo.com/32851190>]

Resource : <http://www.hirensbootcd.org/>

making this tutorial have taken me about an hour to read and format and it will only take 10 seconds from you to say thanks.

Thanks for Reading,
Null

Rolex? - September 8, 2014, 10:05 am

Yeah I always have a hirens boot usb on me. It has tons of features.

Vaxorr - September 8, 2014, 10:10 am

(Sep 8, 2014 10:05 AM)HgB Java Wrote: [\[CITE\]](#) Yeah I always have a hirens boot usb on me. It has tons of features.

yeah i never i always wanted something like this

Mutiny - September 10, 2014, 1:38 am

does this work for windows 8 ? I still am trying all of these things and they dont work since I lost admin

eklat92i - September 11, 2014, 4:55 am

Thanks for this tut i will try this soon !

cl@usi - September 11, 2014, 5:21 am

Try kon-boot it should be on that disc too. And btw. Hirens CD is a bit obsolete, you should use Falcons 4 Boot CD which seems to be still updated.

