

Forum:[Hack Forums](#)

Thread: [get/change admin password](#)

smallz - December 18, 2009, 11:04 am

This tutorial may be on here however I have not seen it. So here it is. Say you are locked out of a system (it can be running xp,vista,7,NT platforms server 2003 etc) Then you can get into the sam files which is where the passwords are stored and change the admin password to "blank" or change it to a password of your liking.

1. We want to go here:

<http://pogostick.net/~pnh/ntpasswd/bootdisk.html>

Now once you get to the site goto the bottom of the page and download cd80802.zip this is the iso for the program we need.

2. Once downloaded upzip the iso to your desktop and then open up your burner and burn this .iso to a cd. once the cd is burned we are almost ready.

3. Now the computer that you are locked out of, you need to turn the power on and press "F8" to change boot order, you want to change the boot order for your cd rom to load first, put your disk you just made in and restart.

4. Now our program we just burned will automaticly load. Once it is loaded it will say Boot: press enter (it will now load drivers)

5. The next prompt will say "select disk where windows installation is" you will press enter here as well and it will show you a list of drives and next to the drive that has your operating system installed on it should say boot if you have more than one drive that says boot then type in "L" this will give you the most probable partition that windows is installed on. if its drive 4 then press 4 if its 2 then press 2

6. Now it will try to mount the system, if it says can not mount would you like to force mount, do not panic just press "Y" for yes and then you will move onto the next step

7. next will say "select which part of registry to load" select "1" which is password reset this will open the chntpw main screen

8. it will look like this

```
===== chntpw Main Interactive Menu =====
```

Loaded hives:

- 1 - Edit user data and passwords
- 2 - Syskey status & change
- 3 - RecoveryConsole settings
- - -
- 9 - Registry editor, now with full write support!
- q - Quit (you will be asked if there is something to save)

What to do? [1]

press 1, then you will see this

===== chntpw Edit User Info & Passwords =====

RID	Username	Admin?	Lock?
03e8	admin	ADMIN	
01f4	Administrator	ADMIN	dis/lock
03ec	grumf1		
03ed	grumf2		
03ee	grumf3		
01f5	Guest		dis/lock
03ea	jalla1	ADMIN	BLANK
03eb	jalla2		BLANK
03e9	petro	ADMIN	BLANK

it will then say select user [administrator] hit enter

then you will get 4 options:

1. clear password to "blank"
2. change password
3. promote user (which will let you promote any user to admin)
4. unlock and enable (if you have tried to login to the user account to many times it will lock you out if it says dis/lock next to admin like above does then you will need to select option 4 and then option 1 to change password.

9. now you are done you need to press "!" to quit, it will then ask if you want to what you want to do, type "Q" for wuit

10. it will say do you want to write back changes do it: type "Y" if you do not write back your changes will not be saved. once done take disk out and hit control alt delete to restart and once login screen comes up you can now login by pressing enter (because you made the pw field blank) or type in the password that you changed it to

I have tested this one 2 out of my 5 computers, and your best to change the password to "Blank" because the change password option does not work all the time but the blank option does work all the time, and once you login you can change the password to what you want to change it to.

sorry this tut is so long and disorganized. hope this helps

sunmaungoo - December 19, 2009, 9:20 am

It help man,thank.You help me out.

smallz - December 19, 2009, 12:30 pm

no problem, sorry the tut was so un organized, but atleast you followed it

momwasscammed - August 26, 2015, 11:29 am

Hi, I just joined this forum because a google search brought up your post linking to cd80802. I went to the webpage link in step 1 of your tutorial because I need to download cd80802, but I couldn't find cd80802.

My mom was scammed into letting someone install a startup password (syskey) on her windows xp device, and without startup password we can not even boot into safe mode.

I am following a tutorial on how to remove syskey and administrator password which requires the use of cd80802

Can you help me find cd80802? Thank you.