Recover the password of the 'Log On' account in windows XP

For many reasons you may lose the password of your Windows login account (due to forgetting, due to unintended changes), what should you do? If the account forgets the password as Administrator, the way to remove it is more complicated. You use the Offline NT Pas tool

For many reasons you may lose the password of your Windows login account (due to forgetting, due to unintended changes), what should you do?

If the lost password account does not have the highest administrator rights, you can log in to an Administrator account to change it. Specifically, the steps are to access *Control Panel -> User Accounts* -> select account to *Reset* password then select " *Change the password* " or " *Remove the password* " is successful.

If you forget the password of the non-Administrator account . You can fix it yourself by the following way:

- Restart the computer and when Windows displays the Logon screen, press *Ctrl + Alt + Del* twice, another login screen will appear. In the *Username* section, type in Administrator. And the *Password* entry is left blank and then press *Enter* . Normally when installing Windows, the password of the Administrator account is usually left blank so you can use the above method to login to Windows

- After logging into Windows, right-click *My Computer -> Manage* . An admin window pops up, select *Local*

Users and Groups -> Users . On the right will show a list of all the accounts in your computer. Select the account you forgot your password, right-click and choose *Set Password* . Then re-enter the new *Password* for that account and then click *OK* .

- Restart the computer and log back in with the new password.

If the account has forgotten password, Administrator is more complicated to remove. You can use *Offline* tool *NT Password & Registry* of Pnordahl to reset the Administrator account password in a simple and effective way.

This tool applies to Windows 2000, XP, and 2003 operating systems running FAT32 and NTFS file format systems and you only need to have a floppy disk.

The way this tool works is to use the minimum boot files of the Linux operating system and perform access to SAM *(% Systemroot% System32configSAM*) which stores the user's passwords in the Windows operating system. , then run the command to Reset the password. Download this tool to your computer at the following address: http://home.eunet.no/~pnordahl/ntpasswd/bd050303.zip

Steps to create a floppy disk to perform :

- Insert the floppy disk into the drive
- Run the *install.bat* file
- Enter the floppy drive name at the prompt: " *Enter target diskette drive:* " (usually A :)

Then wait for the tool to proceed to copy the necessary files to the floppy disk. After copying the alarm system press any key to finish and we have the soft disk containing the tool to perform.

Steps to reset the password

Insert the floppy disk into the computer to Reset the password and boot from the floppy.
Wait for the system to start and after starting us to the on-screen to perform

Which disk contains your Windows system?
== =======
. Step ONE: Select disk where cài ??t Windows
== =======
Disks:
Disk / dev / ide / host0 / bus0 / target0 / lun0 / disc: 2147 MB, 2147483648 bytes
NT found partitions:
1: / dev / ide / host0 / bus0 / target0 / lun0 / part1 2043MB Boot

Hãy ch?n phân vùng b?ng s? hay
a = show all phân vùng, d = t? ??ng n?p new disk drivers
m = manually load new disk drivers
l = relist NTFS / FAT partitions, q = quit
Select: [1]

At this screen, the tool automatically detects partitions on the system hard disks and we simply select the partition where Windows is installed. (In this situation we choose 1) Next screen shows options for execution.

Selected 1
Mounting on / dev / ide / host0 / bus0 / target0 / lun0 / part1
NTFS volume version 3.1.
Filesystem is: NTFS
== =======
. Step TWO: Select PATH and registry files
== =======
What is ???ng d?n vào th? m?c registry? (t??ng ??i v?i ??a Windows)
[windows / system32 / config]:
-r -------- 1 0 0 262144 Jan 12 18:01 SAM
-r -------- 1 0 0 262144 Jan 12 18:01 SECURITY
-r -------- 1 0 0 262144 Jan 12 18:01 default
-r -------- 1 0 0 8912896 Jan 12 18:01 software
-r -------- 1 0 0 2359296 Jan 12 18:01 system
dr-x ------ 1 0 0 4096 Sep 8 11:37 systemprofile
-r -------- 1 0 0 262144 Sep 8 11:53 userdiff
Ch?n ph?n c?a máy ph?c v? ?? n?p, dùng tùy ch?n tùy ch?n
ho?c danh sách các t?p tin v?i ch? nh? m?t delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[first] :

Select 1 to perform *Reset password* and the next screen will appear as follows

== =======
. Step THREE: Password or registry edit
== =======
chntpw version 0.99.2 040105, © Petter N Hagen
[. some info here .]
* SAM policy limits:
L?i logins tr??c khi m? khoá là: 0
Minimum password length: 0
Password history count: 0
> ======== > 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] -> 1

Continue to select 1. That screen will show the system's users

What to do? [1] -> 1
===== chntpw Edit User Info & Passwords ====

RID: 01f4, Username:
RID: 01f5, Username:, * disabled or locked *
RID: 03e8, Username:, * disabled or locked *
RID: 03eb, Username:

, * disabled or locked *
RID: 03ea, Username:, * disabled or locked *
Select:! - quit,. - list users, 0x - User with RID (hex)
or simply enter username to change: [Administrator]

In this case our device is using the *User Administrator*, we click *Enter* to select. (You can choose another *User* to *Reset* by typing that User's name) and the next screen is as follows:

RID: 0500 [01f4]
Username: Administrator
fullname:
comment: Built-in account for administering the computer / domain
homedir:
Account bits: 0x0210 =
[] Disabled | [] Homedir req. | [] Passwd not req. |
[] Temp. duplicate | [X] Normal account | [] NMS account |
[] Domain trust ac | [] Wks trust act. | [] Srv trust act |
[X] Pwd don't expir | [] Auto lockout | [] (unknown 0x08) |
[] (unknown 0x10) | [] (unknown 0x20) | [] (unknown 0x40) |

??ng nh?p ??ng nh?p ??ng nh?p: 0, trong khi quá th? là: 0
Total login count: 3
* = blank password (This may work better than setting a new password!)
Hãy nh?p không nào ?? thoát nó không
Please enter new password: *

At this screen, enter a new Password for the chosen User administrator (go to select * to Reset the password to white - this is recommended by this program). Then the system asks if you really want to Reset the password

Do you really wish to change it? (y / n) [n] y

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] -> q

Select **Y** to agree and wait a bit for the tool to proceed. The screen will then return to the options. Select q to finish the Reset process and the next screen will appear as follows and continue to choose y to finish.

Hives mà ?ã thay ??i:

Name
0 - OK
== =======
. Step FOUR: ?ang ghi back thay ??i
== =======
About ?? ghi t?p tin (s) back! Do it? [n]: y
THIS IS YOUR LAST CHANCE! N?u b?n tr? l?i y ?ây có s? ???c m?t ghi vào ??a!
Writing sam

NOTE: A fixup disk s? NOW ???c th?c hi?n . nó có th? có m?t th?i gian

Mounting volume . OK
Processing of $ MFT and $ MFTMirr completed successfully.

Version NTFS volume is 3.1.

Flags c?n thi?t trên phân vùng . OK

?ang ??n tr?ng c?a t?p tin ($ LogFile) . OK

Partition NTFS / dev / ide / host0 / bus0 / target0 / lun0 / part1 was processed successfully.
NOTE: Windows will run a diskcheck (chkdsk) on next boot.
NOTE: này là ?? xác ??nh b? phân vùng ??a sau các thay ??i

***** EDIT COMPLETE *****
B?n có th? th? l?i If nó b? l?i, ho?c b?n ?ã ch?n không ?úng
New run? [n]: n

Finally, select n when the tool asks you if you want to perform the process again, and then re-launch the floppy. And now User administrator has a blank password and you continue to log in to the normal system.

Note: In addition to performing on the disk, you can create a CD to perform the above operations. To create a CD, please refer to http://home.eunet.no/~pnordahl/ntpasswd/

xhtt911@gmail.com
(The article has reference of **Nguyen Van Viet**)