

KH.CO SOFTWARE



WWW.KH-CO.BLOGFA.COM

Hacking Windows XP Password



By: Khashayar Amrahmad (Kh.CO)

Special Thanks From My Best Friend:

Dr.Trojan , IGI , Mr.Invisible , Lord_Delta , Mr.Amir , And ...

Official Web Site: www.kh-co.blogfa.com

Our Web : www.forum.iranled.com

E-Mail: kh.super.nova@Gmail.com

Y! ID : sabotage_virus@Yahoo.com

**In This E-Book You Learn How To Hacking Windows XP Password
Complete Hacking With Software's And Other Tools In Windows**

You Can Hack XP Password In 5 Minutes



Attention:

**This E-Book Just For Learning You To Get Your Password If You
Forgot Your XP Password
Don't Abuse It**

Not For Sabotage Work



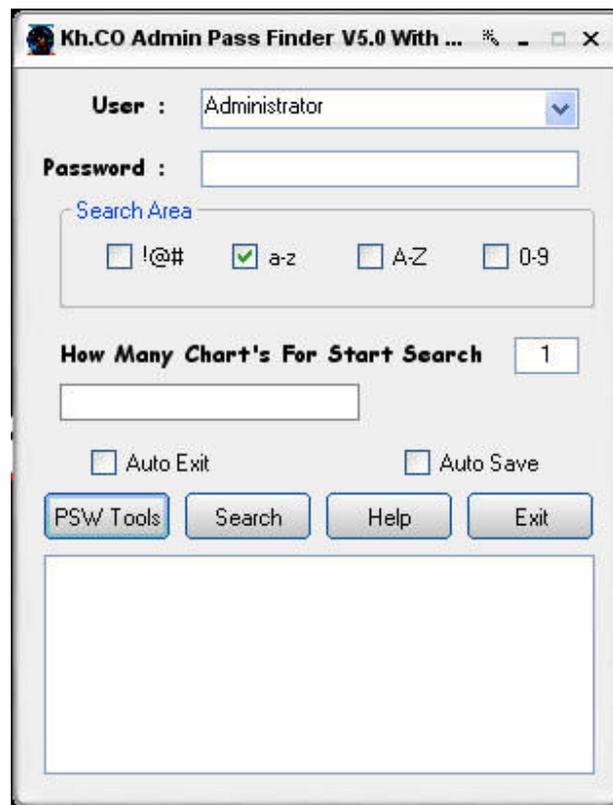
**All Of This Steps And Program Tested In Many Computer
And 100% Worked In All Of Them**



Stage One

Use Kh.CO Admin Pass Finder With Pass Manager

This Software Can Brute Force Attack for Password and Save it in Text File



Finding And Saving Password Might Need Several Minute's
Other Tools In Password Manager :

Get User : Show You Any User In Same Computer With Account Type
(Limit , Ghost , Administrator)

Account Creator: Can Create Administrator User with Password

Password Changer: Can Change Password for Any User (Limit , Ghost
, Administrator)

Delete Account: Can Delete Any User Account with Password

Stage Two Login In Hidden User (**Administrator**)

Before Login Windows You Can Select User You Like To Logged In
In This Place Press ALT+CTRL+DEL Then Wait For New Windows



In This Page You See 2 Text Box

User Name And Password

In User Name Text Box Type : Administrator And Click OK

If Administrator Account Don't Have any Password You Can Login

*In Normal Use Of Computer Administrator Don't Have Password *

In Administrator User You Can Edit ,Delete , Create And Change
Account And Other Configuration

Attention !!!

This Account Have Full Access Control In Computer

Don't Abuse It

:D

Stage Three

Using **Command Prompt (Dos)**

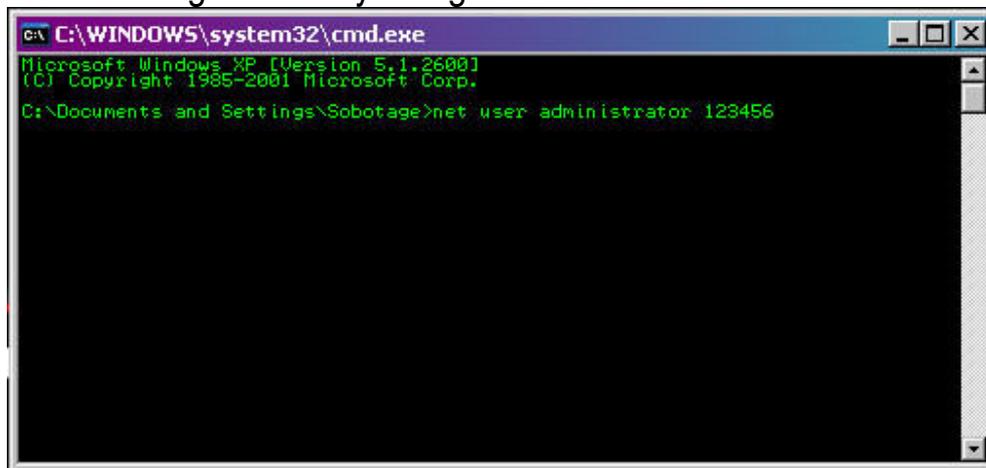
You Can Change Or Create Password From Command Prompt In Windows

Use This Command For Changing Administrator Password :

"Net User Administrator 123456"

"Administrator" Is Password And "123456" Is Password

You Can Change It To Any Things



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Sobotage>net user administrator 123456
```

For Deleting Account Use This Command :

"Net User Administrator /Del"

For Creating Account Use This Command :

"Net User Administrator2 /Add"

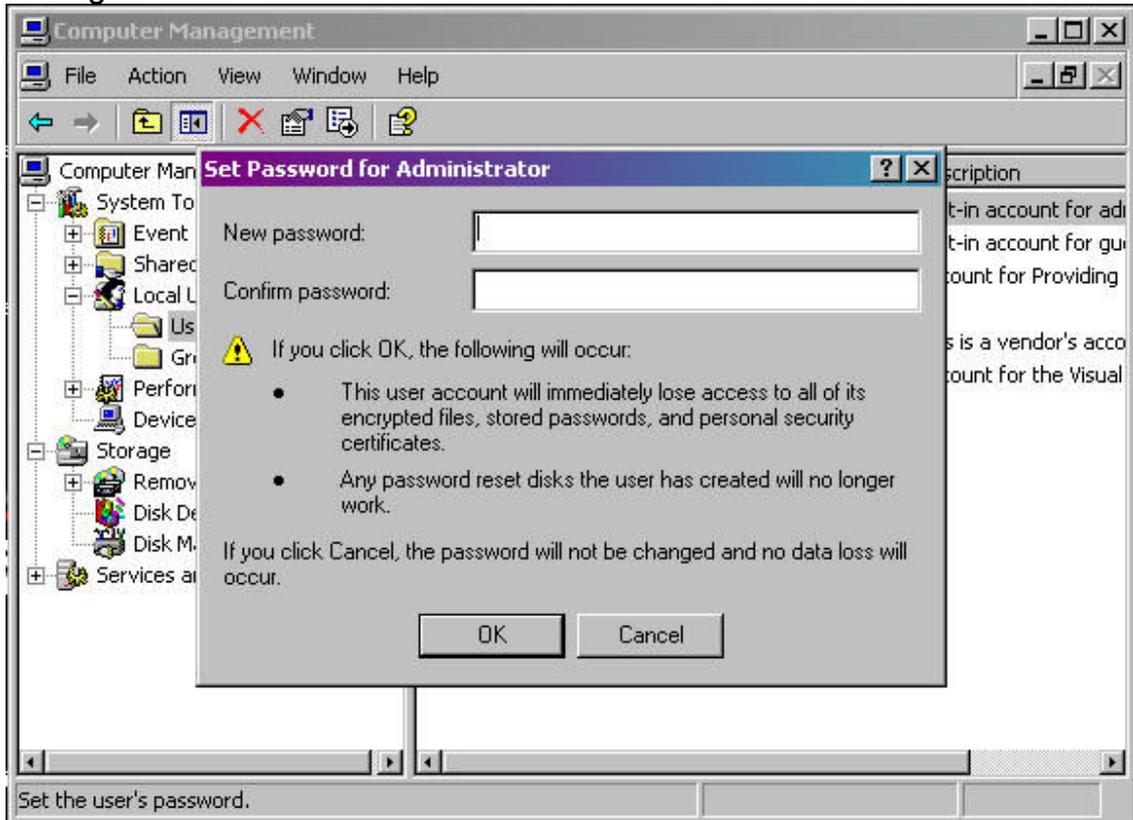


```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Sobotage>net user khashi /add
The command completed successfully.
C:\Documents and Settings\Sobotage>net user khashi /del
The command completed successfully.
C:\Documents and Settings\Sobotage>
```

Stage Four

Using **Windows Manager**

You Can Use Windows Manager To Create , Delete , Change Type, Change Password And ...



On Desktop Right Click On **My Computer** Then Click On Manage
In Manager Click On **Local Users And Groups** , In **Users** Folder
See All User And Account Type ,Right Click On Administrator Then
Select **Set Password ...** After Viewing Information (About Resetting
Password And Crashing System After Changing Password And Other
Problem After Changing Process)

Click On Proceed

In New Windows You Can Set New Password For Administrator

You Can Change Type Of Account In Properties Of Any Account
In "Member Of" Tab

You Can Add Or Change Account Member

Stage Five

Using Active@ Password Changer

You can select the type of search for Security Accounts Manager (or SAM) database in your system

```
Active@ Password Changer v.3.0 (build 0277)

OPTIONS:

1 Choose Logical Drive
2 Search for MS SAM Database(s) on all hard disks and logical drives
3 Exit

Your choice: [_]

Press Esc to exit

1999-2005 (C) Active Data Recovery Software      www.password-changer.com
```

Program displays all logical drives in your system, so you can choose the specific logical drive for SAM database search

```
Active@ Password Changer v.3.0 (build 0277)

Logical drives list:

No:HDD:Partition: Type      : Disk Label: Size (Mb)
-----
0 (0)      (0)      FAT16      BO OT      203
1 (0)      (1)      NTFS       WIN2K      4902
2 (1)      (0)      FAT16      P_FAT      996
3 (1)      (1)      FAT32      P_FAT32    996
4 (1)      (2)      NTFS       P_NTFS     996
5 (1)      (3)      NTFS       BIGCLUSTER 1106

Your choice (0..5 or All)[A]: [1]

Press Esc to exit

1999-2005 (C) Active Data Recovery Software      www.password-changer.com
```

You can see the search results for the security databases. You can select the proper SAM database

```
Active@ Password Changer v.3.0 (build 0277)

MS SAM Database(s) on all Logical drives:

No:HDD:Partition: Type      : Disk Label: MS SAM Database Path
-----
0 (0)      (0)      FAT16      BO OT      \WIN_C\SYSTEM32\CONFIG\sam
1 (0)      (0)      FAT16      BO OT      \TEST\WIN\SYSTEM32\CONFIG\sam
2 (0)      (0)      FAT16      BO OT      \USER\WIN\SYSTEM32\CONFIG\sam
3 (0)      (0)      FAT16      BO OT      \ANT\SYSTEM32\CONFIG\sam
4 (0)      (0)      FAT16      BO OT      \INI_WI^I\SYSTEM32\CONFIG\sam
5 (0)      (0)      FAT16      BO OT      \INI_WI^2\SYSTEM32\CONFIG\sam
6 (0)      (1)      NTFS       WIN2K      \WINNT\SYSTEM32\CONFIG\sam
7 (1)      (0)      FAT16      P_FAT      \WIN_F\SYSTEM32\CONFIG\sam
8 (1)      (0)      FAT16      P_FAT      \WIN_C\SYSTEM32\CONFIG\sam

There are 9 MS SAM databases detected. Choose the one to process.
Your choice (0..8)[0]: [1]

Press Esc to exit

1999-2005 (C) Active Data Recovery Software      www.password-changer.com
```

After SAM database selection you will see the local user accounts list. Built-in local Administrator account is always on top of this list and is outlined by CYAN color

```
Active@ Password Changer v.3.0 (build 0277)

                                USER LIST
MS SAM path: \WINNT\SYSTEM32\CONFIG\sam          Total users: 0087
at disk(0)partition(1)Label<WIN2K>, FS: NTFS

-----
No:  RID  !User Name      ! Description
-----
0 000001f4 Administrator  Built-in account for administering the comp
1 000003e8 puv           Senior Admin
2 000003f2 RWhite        Network systems engineer (IT Department)
3 000003f3 MBrown        User support (level 1)
4 000001f5 Guest         Built-in account for guest access to the co
5 000003ec RBartolucci  CIO
6 000003ed LDombrowsky  Field engineer
7 000003ee EParsons     UrbanSoft Inc., Vice President
8 000003ef MMeilleur    Liberal MPP for Ottawa-Vanier and Minister
9 000003f0 RPatten     RTA Business division security officer

Your choice: [2]
Press Esc to exit or PgUp/PgDown to scroll User List

1999-2005 (C) Active Data Recovery Software          www.password-changer.com
```

A detailed user's account information is displayed on the screen. It is possible to accept or to change default settings in the right column. You take a decision - to reset a password for this user account or not

```
Active@ Password Changer v.3.0 (build 0277)

                                User's Account parameters:
MS SAM Database: (0)(1)<WIN2K>\WINNT\SYSTEM32\CONFIG\sam

Full Name : "Karoline White"
Description: "Network systems engineer (IT Department)"
Existing: Change to:
[ ] [ ] User must change password at next logon
[X] [X] Password never expires
[ ] [ ] Account is disabled
[ ] [ ] Account is locked out
[ ] [X] Clear this User's Password

PgDn to view or/and change permitted logon hours

Press Y to save changes and exit or Esc to exit without saving

1999-2005 (C) Active Data Recovery Software          www.password-changer.com
```

"Success" message is displayed after the local user's password has been successfully reset

```
Active@ Password Changer v.3.0 (build 0277)

                                User's Account parameters:
MS SAM Database: (0)(1)<WIN2K>\WINNT\SYSTEM32\CONFIG\sam

Full Name : "Karoline White"
Description: "Network systems engineer (IT Department)"
Existing: Change to:
[ ] [ ] User must change password at next logon
[X] [X] Password never expires
[ ] [ ] Account is disabled
[ ] [ ] Account is locked out
[ ] [X] Clear this User's Password

PgDn to view or/and change permitted logon hours

Press Y to save changes and exit or Esc to exit without saving
User's attributes has been succesfully changed. (Press any key...)

1999-2005 (C) Active Data Recovery Software          www.password-changer.com
```

Complete Hacking Windows XP

Thanks To All Helper :

Dr.Trojan , IGI , Mr.Invisible , Ha_60 , Mr.Amir And Other Friend

Special Thanks To :

Black Code , Linux Kernel , Hell Bound Hacker , Login Recovery , Delta Team , Iranvig , And Other Team's And Web Site

Written By : Kh.CO

Sabotage_Virus@Yahoo.com

Kh.super.nova@Gmail.com

www.kh-co.blogfa.com



(~) My Dream Is Girl Standing In The Sun (~)