OPEN SOURCE

Reset Windows passwords with the help of Linux

One cost-effective and reliable way to reset a Windows password is to keep a copy of Linux with you and use the chntpw application.

By Jack Wallen | in TR Dojo, July 17, 2012, 6:04 AM PST

You lose your Windows password(s) and cannot log in to your machine. If you have a rescue disk, you should be okay. If not, you might have to turn to Linux for help.

The method that I describe in this tutorial can work with a Windows machine that either dual boots with Linux or does not. If the machine in question does not dual boot, you will need to download a live edition of a Linux distribution (I prefer Ubuntu (http://www.ubuntu.com/) for the task) and burn that ISO image to a disk (you could also use a Linux distribution on a USB drive). Either way, you will need to boot in to Linux to recover your password.

Step 1: Boot in to Linux

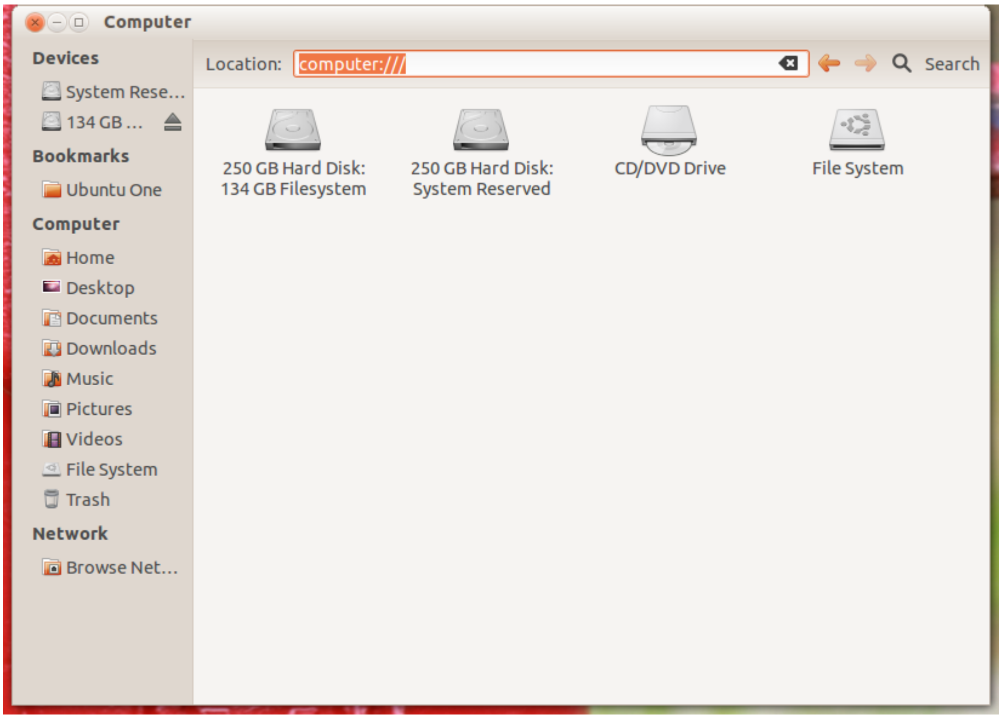
Put the burned disk in the drive (or boot from USB) and boot in to the Live edition of Linux. You should use the standard Live session.

Step 2: Find the Windows partition

Open Nautilus (the GNOME file manager) and follow these steps:

1. Hit the Ctrl-L key combination to open the Location bar (**Figure A**).
2. Enter the string "computer:///" (no quotes).
3. Locate the drive (or partition) that contains your Windows installation.
4. Right-click the Windows drive icon and click Mount.
5. Double-click the icon to open the Windows drive (or partition) and make note of where the drive is mounted (it will be listed in the location bar).

Figure A



Location: computer:///

(https://tr1.cbsistatic.com/hub/i/2015/05/07/c0a7b735-f48e-11e4-940f-14feb5cc3d2a/nautilus_1.png)

The drive in question on my system is the far left icon. (Click the image to enlarge.)

Step 3: Get to the command line

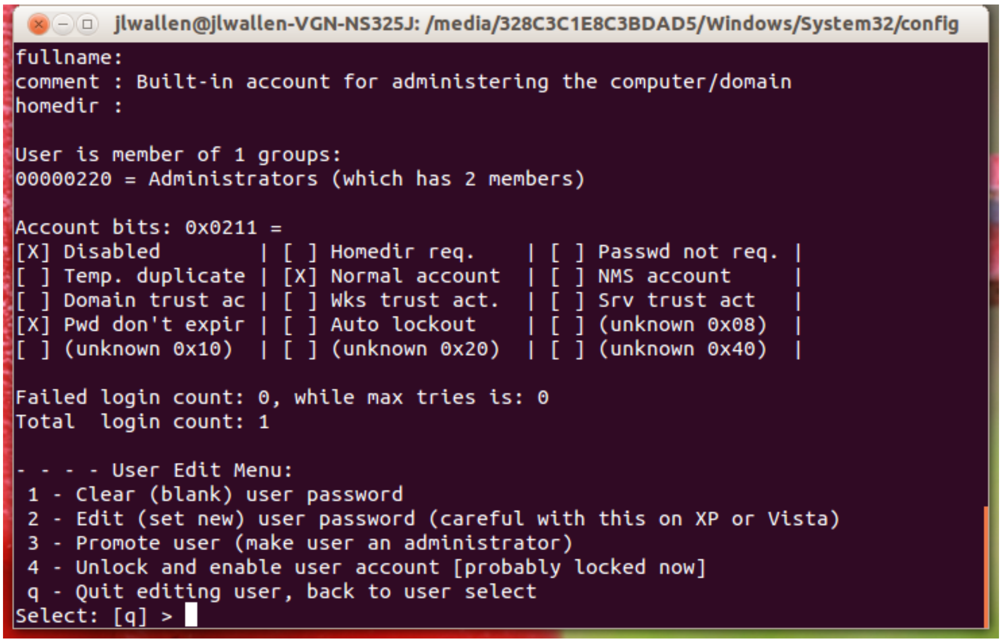
It's time to open a terminal window and begin (or continue) your journey into the Linux command line. You must install the small tool called *chntpw*. To install this application, issue the command: *sudo apt-get install chntpw*. With that application installed, you are ready to go. Follow these steps to get the password changed:

1. Change into the directory containing Windows with the command *cd /PATH/TO /WINDOWS* (PATH/TO/WINDOWS is the complete directory path to your Windows drive).
2. Change into the Windows/System32/config directory.
3. Issue the command *sudo chntpw SAM*.

You should now see the chntpw screen (**Figure B**). Here you have five options:

- Clear user password
- Edit user password
- Promote user (make user an administrator)
- Unlock and enable user account
- Quit

Figure B



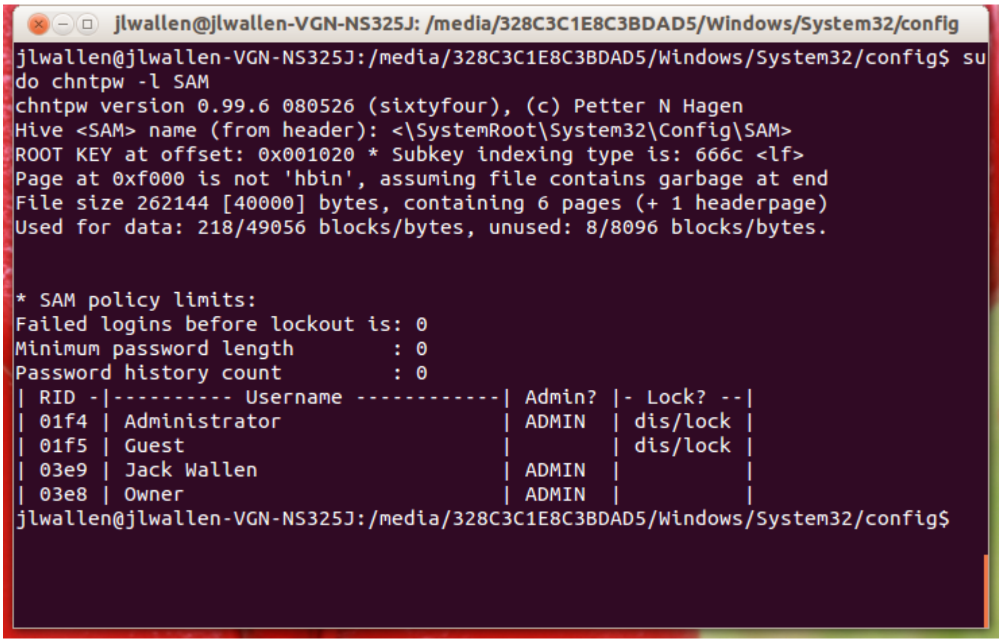
jlwallen@jlwallen-VGN-NS325J: /media/328C3C1E8C3BDAD5/Windows/System32/config

```
fullname:
comment : Built-in account for administering the computer/domain
homedir :

User is member of 1 groups:
00000220 = Administrators (which has 2 members)

Account bits: 0x0211 =
[X] 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)  |

Failed login count: 0, while max tries is: 0
Total  login count: 1

- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
 4 - Unlock and enable user account [probably locked now]
 q - Quit editing user, back to user select
Select: [q] >
```

(https://tr1.cbsistatic.com/hub/i/2015/05/07/c121fc94-f48e-11e4-940f-14feb5cc3d2a/chntpw_1.png)

You do not want to make changes here, because this could wipe all users' passwords — make sure you are working with a specific user. (Click the image to enlarge.)

Enter "q" for quit. We're going to make sure we are working with a specific user. To list out all users in the SAM file, issue the command *sudo chntpw -l SAM*. This will list out all of the users on the system. As you can see in **Figure C**, my name is listed as one of the users. **Figure C**



jlwallen@jlwallen-VGN-NS325J: /media/328C3C1E8C3BDAD5/Windows/System32/config

```
jlwallen@jlwallen-VGN-NS325J:/media/328C3C1E8C3BDAD5/Windows/System32/config$ su
do chntpw -l SAM
chntpw version 0.99.6 080526 (sixtyfour), (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
Page at 0xf000 is not 'hbin', assuming file contains garbage at end
File size 262144 [40000] bytes, containing 6 pages (+ 1 headerpage)
Used for data: 218/49056 blocks/bytes, unused: 8/8096 blocks/bytes.


* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length        : 0
Password history count         : 0
| RID -|---------- Username ------------| Admin? |- Lock? --|
| 01f4 | Administrator                  | ADMIN  | dis/lock |
| 01f5 | Guest                          |        | dis/lock |
| 03e9 | Jack Wallen                    | ADMIN  |          |
| 03e8 | Owner                          | ADMIN  |          |
jlwallen@jlwallen-VGN-NS325J:/media/328C3C1E8C3BDAD5/Windows/System32/config$
```

(https://tr1.cbsistatic.com/hub/i/2015/05/07/c197946b-f48e-11e4-940f-14feb5cc3d2a/chntpw_2.png)

This listing will also tell you how many failed login attempts have been made. (Click the image to enlarge.)

To work with a specific user, issue the command *sudo chntpw -u "USER NAME" SAM* (USER NAME is the actual username). If the username is only one word, you will not need the quotes. If the username is a full name, place it within quotes or the command will not work. Once you are back in the edit screen, do the following:

1. Type "2" (no quotes) to go into edit mode.
2. Type the new user password.
3. Hit the Enter key.
4. Type "y" (no quotes) followed by Enter to write the file.

Your Windows User password should be changed. Reboot into Windows to make sure the edit worked. If it did not work, go through the steps once again and, this time, blank the password instead of editing it. To blank the password, do the following:

1. Enter the edit screen for the specific user.
2. Type "1" (no quotes).
3. Hit Enter.
4. Type "y" (no quotes).
5. Hit Enter.

At this point the user account should have no password. You can reset the password once you successfully log in to Windows.

RELATED TOPICS: SOFTWARE SECURITY DEVELOPER ENTERPRISE SOFTWARE INNOVATION

About Jack Wallen

Jack Wallen is an award-winning writer for TechRepublic and Linux.com. He's an avid promoter of open source and the voice of The Android Expert. For more news about Jack Wallen, visit his website jackwallen.com.

Teach your users how to create strong passwords with our tutorial

IBM's Space Rogue explains how hackers easily crack your password

Microsoft drops Edge browser into iOS and Android for free

ADD YOUR COMMENT

WHITE PAPERS, WEBCASTS, AND DOWNLOADS

EDITOR'S PICKS

NASA's unsung heroes: The Apollo coders who put men on the moon

Elon Musk and the cult of Tesla: How a tech startup rattled the auto industry to its core

Cyberweapons are now in play: From US sabotage of a North Korean missile test to hacked emergency sirens in Dallas

FREE NEWSLETTERS, IN YOUR INBOX

Tech News You Can Use

We deliver the top business tech news stories about the companies, the people, and the products revolutionizing the planet.

Delivered Daily

✉ SUBSCRIBE

Best of the Week

Our editors highlight the TechRepublic articles, galleries, and videos that you absolutely cannot miss to stay current on the latest IT news, innovations, and tips.

Delivered Fridays

✉ SUBSCRIBE