Resetting the Local Administrator Password

You can reset the local administrator password on a Win2k or WinXP[1] computer using a program called chntpw.

- http://freshmeat.net/projects/chntpw/

Description from the Web…

> chntpw is a utility to (re)set the password of any user that has a valid (local) account on your NT system, by modifying the crypted password in the registrys SAM file. You do not need to know the old password to set a new one. It detects and offers to unlock locked or disabled out user accounts! It works offline, that is, you have to shutdown your computer and boot off a floppydisk or CD. The bootdisk includes stuff to access NTFS partitions and scripts to glue the whole thing together.

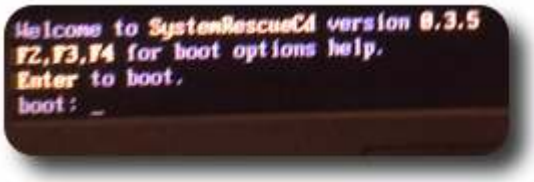
We will be using this program from the bootable Linux CD called SystemRescue-Cd. This allows us to mount the NTFS partition with read/write access.

- http://www.sysresccd.org

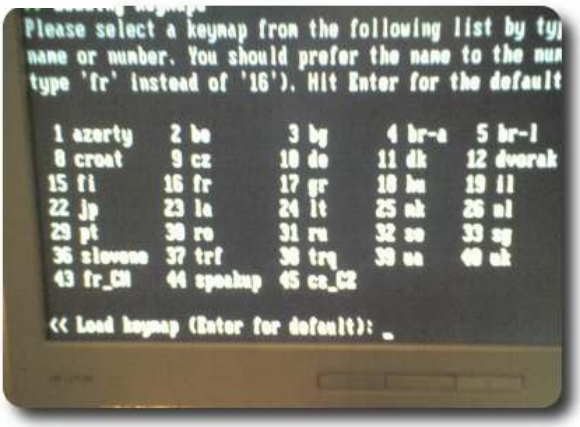
Required:

- Physical access to the PC
- PC set to boot from CD
- SystemRescue-Cd ver.0.3.5 or greater

1. Put the SystemRescue-Cd in the CD-Rom drive and reboot the PC
2. When the PC has booted from the CD you will see the 'boot:' prompt, press Enter



3. At the 'Load keymap' press Enter for default



[1] As of this writing I have not tested with Vista

4. When you are fully booted you will be at a prompt starting in the root directory (/root %)

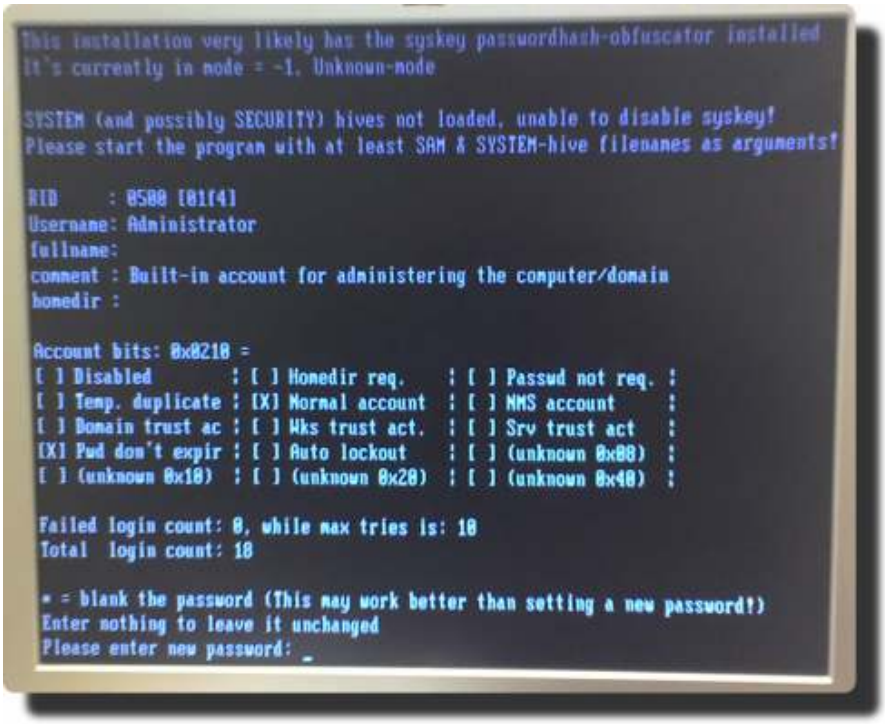
5. mount the Windows system partition in read/write mode
   - type in the following at the command line
   - ntfs-3g /dev/hda1 /mnt/windows

   - the Windows system partition is now read/write enabled

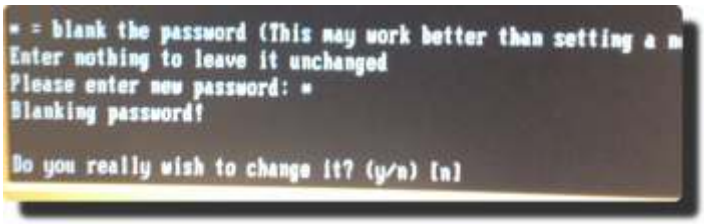
Change to the mounted 'windows' drive and the location where the registry files are; enter at the command line…

1. cd /mnt/windows/WINNT/system32/config
2. Your command line prompt should now look like this…
   17:11 /mnt/windows/WINNT/system32/config % _
3. At this command line type in **chntpw SAM**

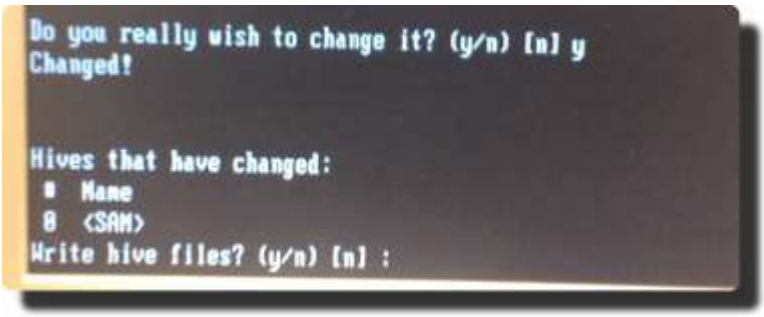
4. This defaults to the local machines administrator account
5. The next prompt asks you for a new password. For best results set it to a blank password by entering a * and pressing enter.



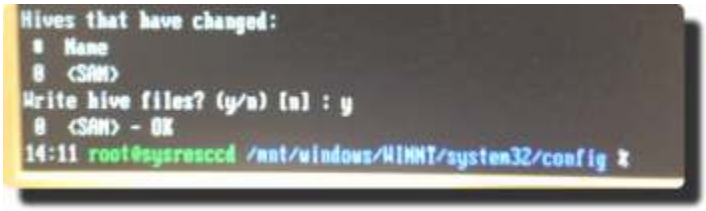
6. You will be prompted 'Do you really wish to change it?' , reply 'y' and press enter



7. Then you are prompted if you want to 'Write hive files?', reply 'y' and press enter



8. This is followed by a successful confirmation -'**0 <SAM> - OK'**, then you are kicked back to the normal command line



9. Type 'halt' at the command line to get out of Linux.

10. You will see a bunch of text scroll by, when it stops and displays 'System halted. You can turn off your computer", do so

11. Remove the SystemRescue-Cd from the drive
12. Restart the PC to boot back into MS Windows
13. When prompted to logon, use the local administrator account without a password
14. You now have access to the PC