

HOWTO: Recover root password

Contributed by B. Johnson
02-18-06

A common problem faced by new users (and sometimes even experienced users) is not knowing what to do when they lose their password. Even worse, when they lose the password for 'root'. Luckily, there are several solutions to help you recover access to your system.

Root Password - Easy Method:

The simplest way to recover from a lost password is to boot into single user mode.

If you are using LILO, at the LILO boot prompt (graphical LILO users can press Ctrl-x to exit the graphical screen and go to the boot: prompt), enter: Code: linux single

This will make you the "root" user without asking for a password. Once the system has booted, you can change the root password using the passwd command: Code: passwd The instructions for GRUB users are similar. Press 'e' at the GRUB prompt to select boot parameters. Select the line for the kernel you want to boot, and go to the end of it. Add "single" as a separate word, and then press ENTER to exit the edit mode. Once back at the GRUB screen, press "b" to boot into single user mode.

Root Password - Not As Easy Method:

If for whatever reason, the above solution doesn't work for you, there is another option. Boot using a so called "Live CD" Linux distribution, such as Knoppix. For the purposes of this example, it will be assumed that the user is using Knoppix. After booting up from the Knoppix CD, go to a terminal and su to root (no password is required). After your privileges have been escalated, issue the following commands (be sure to replace each /hda1 with your own root ('/') partition):

Code: mount -o dev,rw /mnt/hda1 cd /mnt/hda1/etc

Once you are into your system /etc directory, you can use a text-editor (such as vim, nano, pico, etc.) to edit the /etc/shadow file where the password is stored. Various information about root and user accounts is kept in this plain-text file, but we are only concerned with the password portion.

For example, the /etc/shadow entry for the "root" account may look something like this: Code:

root:\$1\$aB7mx0Licb\$CTbs2RQrfPHkz5Vna0.fnz8H68tB.:/10852:0:99999:7::: (The '/' indicates a line continuation)

Now, using your favorite editor (I'll use vim) delete the password hash (the green text). Code: vim shadow

After you've edited this field, it should look like this: Code: root::10852:0:99999:7:::

Now save the file and change back to the root directory and unmount the system root partition (don't forget to change the /hda1) as follows: Code: cd / umount /mnt/hda1

Now reboot the computer.

Once the computer has booted and you're at the login prompt, type "root" and when asked for the password just press ENTER (entering no password). After a successful login, you need to set the new password for root using the following command: Code: passwd

Forgotten or Lost "User" Password:

If a regular user forgets his/her password, the root user can easily reset the user's password. For this example, the username will be "bob".

Enter (as root): Code: passwd bob

This will prompt for a new password for the user "bob".