

Recovery from an unknown root password

This document contains a Red Hat and SUSE example of recovering from an unknown root password.

On Red Hat



Red Hat systems do not ask for a root password when booting in single user mode. On powered off Red Hat systems the procedure is:

- Boot the computer
- Use `e` in the GRUB boot loader (First press <Escape> in SUSE)
- Use `e` to edit the kernel boot option
- Type `<space> 1` at the end of the line or **'init=/bin/sh'** (also in SUSE)
- Select `b` to enter single user mode
- Use the *passwd* command. You now have a new root user password.



One way to prevent this simple root password recovery method, is to add a password to GRUB.

This procedure will not work on all distributions, because other systems tend to ask a root password for entering single user mode.

Another way to recover from the unknown password is to use *rescue* mode (also see the following objective).

On other systems

On powered off (SUSE) systems the procedure is:



- Boot the computer from the install CD (or rescue diskette)
- Choose *Rescue System* from the boot options. You will be the root user of the booted system without being prompted for a password.
- Mount the / partition of the installed system, e.g.:
 - **mount /dev/hda1 /mnt**
- Make the mounted (installed) system the new root (/) system and change the password of the root user, e.g.:
 - **chroot /mnt passwd**

You **changed** to the installed **root** system and used the **passwd** command to create a new password for the root user.

The command **chroot /mnt** would make the change to the installed system more permanent. E.g. you can change */etc/fstab*, */etc/inittab*, */boot/grub/menu.lst* (The SUSE version of the boot menu *grub.conf*), which are on the installed system until you use the exit command.

If you do not use the *chroot* command, then you would alter the files of the rescue system and not the files of the installed system.



The Red Hat rescue system is similar to SUSE but uses the command **chroot /mnt/sysimage**

Note:

Deleting the x in the */etc/passwd* file of the root entry, removes the password protection for root.

An alternative way to recover from an unknown password is:

- Using a boot CD or USB stick
- Mount the hard disk
- Remove the x
- Restart the system
- Login without a password

Think of a way to enable the password again and if you want to protect your notebook for these actions: Use an encrypted file system (for / or your data partition).