5 tips to improve Linux security

Protecting a networked computer is a challenge that never has an end - even in Linux.

Network Administration **- Protecting a networked computer is a challenge that never ends - even in Linux. These simple methods will help you protect your Linux computers** .

Can you what it? You don't need to do anything about security on a Linux computer just because it is Linux? If you have those thoughts, you need to think again. Linux is an operating system, so it also needs to be protected. Although this operating system can be quite secure, there is no operating system that is 100% safe for all operating times. Here are 5 simple Linux security tips that are very important to this operating system.

1. Take advantage of keyring

For many people, this can be an annoyance. You log on to the computer, the computer requires a connection to a network (or an LDAP server, .) and you must enter your keyring password. This feature can be disabled by giving it a white password and ignoring the warning that you are transmitting unencrypted information (including passwords). However, this is not a good way. Although it may be thought that doing this will increase complexity, the existence of this feature or function has its reasons - it helps to encrypt sensitive passwords when they are sent on line. physical.

2. Execute user password upgrade

If you run a multi-user environment, you need to make sure that your users change their passwords regularly. To do this, you can use the *chage* command. You can check the expiration time with the *sudo chage -l USERNAME* command (here *USERNAME* is the name of the user who wants to check). Suppose you can expire a user password and force him to change it the next time you log on. To do this, you can use the *sudo chage -E EXPLICIT_EXPIRATION_DATE -m MINIMUM_AGE -M MAXIMUM_AGE -I INACTIVITY_PERIOD -W DAYS_BEFORE_EXPIRATION command* (here all options in CAPS are user defined).

3. Do not blindly disable SELinux

Like keyring, SELinux has its own reasons. SE stands for Security Enhanced phrase and it provides an access control mechanism for applications. There are many solutions to solve the problems related to disabling SELinux. However, it actually only makes matters more complicated. If a program does not run properly, you can study changing the SELinux policy to suit your needs instead of disabling SELinux. If you don't want to do this via the command line, you can check the GUI tool called polgengui.

4. Do not log in with the root account

It is not necessary to be strong that Linux users should not log in with a root user account. If you need to perform certain administrative tasks on a computer, log in with regular accounts and *su* for root users or use *sudo* . When logging in as root, you can effectively bypass the mainstream security barrier, allowing access to the system and subsystems that are normally not accessible when logged in as a person. standard use. Do not do this. Log in with your previous account.

5. Install security updates immediately

There is a big difference between how Linux and Windows manage upgrade operations. Windows often makes a major but infrequent upgrade, while Linux performs small upgrades regularly. Ignoring these updates may have serious consequences if the security holes are not patched in time on your system. Remember, one of these upgrades is security patches and should be applied immediately. Never ignore the icon that indicates available updates. And if you are using a server without a GUI interface, set up a script to automatically check for updates or you have to perform a manual check daily or weekly . Constantly updated, then you will be safer.