PLAYING HIDE AND SEEK WITH PASSWORDS

Passwords are used in many ways for security in computers, from BIOS management to logging in to your user account; from accessing hard disk contents, to restricting access to specific services. For Linux, the root password is the most important; if you have it, you own the machine. This article is like a drill, where we break a password, find a way to protect it, and again break it. Who wins? Read on to find out…

We are going to be breaking the root password on an RHEL6 machine. We start with switching to single-user mode. Here are the steps:

1. Press any key as soon as the booting starts. This will display the GRUB menu.

2. Now press e to edit, and go down to the second line, which begins with kernel.

3. Again press e to edit kernel parameters, and at the end of the line, just add a 1 (see Figure 1) to start the system in single-user mode instead of the default run-level.

4. Press Enter to quit kernel parameter editing mode, and then press b to boot the modified options.

5. The system boots to single-user mode; now we just change the root password with the passwd command. If the command doesn't display any output, it indicates that SELinux is in enforcing mode, so we will have to disable it using the setenforce 0 command. Then again run passwd and change the password. After you have changed the password, you can switch to graphical mode using the init 5 command and login to the root account in a terminal, using the newly assigned password.

It's easy to change the root password, isn't it? But this can become a nightmare if someone else does this to your system. So we try to block this approach. Notice that we got access to single-user mode without any password; to patch this hole, we shall require a password to access single-user mode. In RHEL5 you need to write su:S:wait:/sbin/sulogin in /etc/inittab file before id:5:initdefault:. But this doesn’t work in RHEL6. So we edit the /etc/rc1.d/S99single file and write exec /sbin/sulogin before exec init t1 S. Now if you try to switch into single-user mode, you □ll have to enter the root password.

OK can we relax, now that single-user mode is password-protected?

No the game has just begun, and will get more interesting. Here is the next twist: you can still change the root password. In our first go, we edited the kernel parameters to boot into single-user mode. This time we will again play with kernel parameters, but we will instead add init=/bin/bash to the kernel parameters (see Figure 2).

As Figure 3 shows, we try to use passwd to assign a new password but it fails because the / partition is mounted read-only, so the new password cannot be written to the disk. We remount it in read-write mode with mount -o remount,rw / and then use passwd again to change the password. After that, just restart the system; the root account is yours again.

What’s the solution to this problem? We prevent tweaking of kernel parameters in GRUB, by assigning a password to GRUB. Just go to your terminal, run grub-md5-crypt and enter the password you want to apply to GRUB. The utility outputs an encrypted string; select it and copy it. Now edit the grub.conf file and add a line with password–md5 and paste the copied string after that (see Figure 4). Now, to change kernel parameters, you will have to enter this password, as you see in the lower left of Figure 5.

We have almost solved our problem, but there is still a small glitch. We can also remove the password applied to GRUB, by using Linux rescue mode. Set your first boot device to CD, boot the system with the RHEL6 DVD, and select Rescue Installed system. Once you’re in the rescue mode environment, the installed system will be mounted under /mnt/sysimage. Now just run chroot /mnt/sysimage, edit grub.conf (e.g. vim /boot/grub/grub.conf) and delete the password line from it. Save and quit. Now you can get out of rescue mode by entering the exit command twice. Reboot the system (from the hard disk) and you won’t find any GRUB password. The best solution for this problem is to block external devices like CD drive and USB ports, so that an outsider can’t boot with a CD or USB drive.

I hope you ve enjoyed and learnt something through this drill. Do remember that security is not a game; it needs to be strictly applied, intensely monitored and regularly updated to stay ahead of intruders who may try to break into your system.

Source : http://www.opensourceforu.com/2013/03/playing-hide-and-seek-with-passwords/