

Re: Doing administrative work

Source: <http://linux.derkeiler.com/Mailing-Lists/Debian/2007-01/msg03228.html>

- *From:* Douglas Allan Tutty <dtutty@xxxxxxxxxxxxxx>
 - *Date:* Sat, 27 Jan 2007 12:18:46 -0500
-

On Sun, Jan 21, 2007 at 10:03:30PM -0500, Jim Hyslop wrote:

OK, this latest discussion about logging in as root got me thinking. I'm fairly new to Linux. Occasionally, when I need to set up something (as an example, my recent DNS questions) I will need to edit a config file, and restart the daemon. I usually start by logging in as myself, then issue individual 'su [command]' commands. After a while, I get tired of typing in the root password over and over, so I just issue a simple 'su' and work as root from there.

Should I be taking a different approach?

Hi Jim,

As you see from all the replies, the answer is "it depends". To get a specific answer, you need to give specific details on your overall setup.

Personally, for me, I only have two regular users: me and my wife. I have two computers connected via a crossover ethernet cable. Under normal operating procedure, my 486 is just a glorified terminal (via ssh) to my Athlon box. I have an ssh group and only members of ssh can ssh into the box. SSH only listens on the local ethernet port. Only public-key access is allowed. What this means is that the two computers are really, from a security perspective, one computer. If an attacker gains access to one, he gains access to both. Since they are only 20 feet apart in the house its not a huge concern since they could also just pull the backup off the shelf.

I don't log in as root, but run su - when needed. I never run X apps as root. I have pam set up so that only members of group adm (which includes only me) can su.

I could tighten security a lot if I wanted but I'd have to do a lot locally to make it matter. Its all about total risk assessment. The reason that I don't run as root all the time is to protect myself from

Re: Doing administrative work

my own stupid mistakes. I suppose then I could have pam setup so that I don't have to give the root password; typing su gives enough pause. On the other hand, I figure that if I need to su often enough to make this an issue, then I'm doing it too often and would need to look at what I was doing that I couldn't do as myself.

YMMV.

Doug.

--

To UNSUBSCRIBE, email to debian-user-REQUEST@xxxxxxxxxxxxxxxx with a subject of "unsubscribe". Trouble? Contact listmaster@xxxxxxxxxxxxxxxx