

Re: RedHat security

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2002-06/0550.html>

From: Nico Kadel-Garcia (nkadel@bellatlantic.net)

Date: 06/14/02

From: "Nico Kadel-Garcia" <nkadel@bellatlantic.net>

Date: Fri, 14 Jun 2002 11:47:28 GMT

"Yuan Liu" <yliu@stemnet.nf.ca> wrote in message
news:3D097D46.1040606@stemnet.nf.ca...

- > *Nearly every time I set up a RedHat distribution (starting from 6.0)*
- > *anywhere, I find myself asking the same questions. That's why I don't*
- > *usually dare to install RH if its my own system. Generally I'm quite*
- > *confused about its philosophy. Hope someone can shed a light on these.*
- >
- > *1. If someone is physically at the console, he gets total control.*
- > *– No logon for single user stage. I know several commercial Unises (or*
- > *maybe all of them) behave the same. Guess the main reason is for*
- > *password resetting. But Linux can easily be booted using a floppy, so*
- > *if it is truly needed, you can always do this with a rescue disk.*
- > *Though the end result looks the same, the added difficulty provides some*
- > *deterrence, IMO.*
- >
- > *– Anyone, any user can reboot the system. I don't know of another *nix*
- > *doing this and this scares me. I'm on RedHat 7.3 and I don't even have*
- > *to be on a text console; even if I'm in an X-console, I can still do as*
- > *an unprivileged user*

Almost all OS's have this vulnerability. It's certainly possible to put a password on the BIOS, and a password for the boot loader to reduce this ease of access. But I can use boot floppies or media to get into Solaris, BSD, OSF1, and every version of Windows unless you've locked down the BIOS with a password.

- > *\$ reboot*
- > *and send all users to hell. Haven't tested this from a remote session,*
- > *so I group it here. If it also allows any user to do this remotely,*
- > *this is hell proper. Not to mention that the default logon menu has*
- > *this "Reboot" option, just like Windows.*

Most users are not gaining anything from locking down the console further. Honest. If they're sitting there, you'd much rather have them use the "Reboot" icon than hitting the power switch to reset it.

comp.os.linux.security: Re: RedHat security

- > 2. *Anyone can mount/umount a floppy or CD by default. Shouldn't the default be not able to, then allow the admin to grant privilege? And what's wrong with keeping it tight with sudo and stuff?*

It's a bunch of work for minimal benefit. Really. As long as they don't mount suid, it's no more dangerous than copying stuff to their home directory or /tmp/.

- > 3. *Anyone can run, sigh, even grub. Does this scare someone other than myself?*
- >
- > *RH used to have a slew of networking defaults that were not security minded. It seems that they are attacking on them over releases. But these privilege related things are also essential. Looking at what an ordinary user can do in RH makes a full blown virus attack into my dreams – nightmare, is this what such a dream is called? The above are just a few that bothered me most recently. What do you people think?*
- > *Maybe we should start a log or something.*

I think that you should get over this concern. Physical access means control of the machine: you can harden it somewhat with MBR passwords and BIOS passwords, but for most cases it's like locking your car door while driving down the highway: not worth the effort.

-
- **Next message:** www.e-portfolio.co.yu: "----- BERZA IT POSLOVA -----"
 - **Previous message:** [Rex Dieter: "Re: RedHat security"](#)
 - **In reply to:** [Yuan Liu: "RedHat security"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)