

comp.unix.bsd.openbsd.misc: Re: Linux, BSD, and Unix are fundamentally insecure.

Re: Linux, BSD, and Unix are fundamentally insecure.

Source: <http://unix.derkeiler.com/Newsgroups/comp.unix.bsd.openbsd.misc/2004-09/0165.html>

From: Freeride (freeride_at_maillinux.org)

Date: 09/11/04

Date: Fri, 10 Sep 2004 21:13:46 -0700

On Fri, 10 Sep 2004 11:18:44 -0700, Mike Cox wrote:

- > *That's not what he did. You don't understand *nix if you don't know*
- > *that everyone of those commands is needed. The box was not logged in*
- > *to, it had the login prompt there. Scott rebooted (ctrl alt del) the*
- > *machine and passed a command to GRUB that booted linux into the BASH*
- > *shell. He then mounted the /proc file system and then the / filesystem.*
- > *He then changed the password.*
- >
- > *Every *nix machine is vulnerable to this sort of local security flaw. If*
- > *you password protect the BIOS to prevent this, someone can just take out*
- > *the battery out of the PC and then the BIOS password is reset. Someone*
- > *can just take the Linux disk out, boot their own system and mount your*
- > *disk no problem.*
- >
- > *Windows doesn't have this flaw. It requires the Administrator password*
- > *before it will let you into safe mode or use the Windows 2000 recovery*
- > *CD.*

Bullshit!!

<http://www.winternals.com/products/repairandrecovery/erdcommander2002.asp?pid=erd>

ERD Commander 2003.

(Includes the Locksmith utility to reset lost Administrator passwords)

Can boot any Winders box from a CD reset the admin password.

- > *If you use the NTFS filesystem, you can select to encrypt the hard drive*
- > *filesystem. That prevents someone from taking the disk out and trying*
- > *to mount it using another OS.*

Again I can boot the system up with ERD and change any users password then boot up Windows and un-encrypt any of those file! Can also snag the certificate that was used to encrypt those files.

- > *If you have*
- > *encryption enabled, and mount a Windows disk on Linux, you wont be able*

Re: Linux, BSD, and Unix are fundamentally insecure.

comp.unix.bsd.openbsd.misc: Re: Linux, BSD, and Unix are fundamentally insecure.

> *to get in.*

Wow you almost sound knowledgeable.

> *I've tried it. Heck, once i've forgotten my Windows
> 2000 Admin password and was locked out forever.*

Because your a moron.

> *But not with Linux.
> Forget you root password, and you can get a new one in about 1 minute.
> Not very secure.*

Nothing that you have physical access to is secure.

> *Not ready for the enterprise.*

What the fsck do you know about enterprise computing.

> *And a BIOS password is not a fix. Someone can just take the battery out
> of the PC and it is reset.*

Again you are taking out your ass. Many of the new systems/server have highly protect bios password capabilities, and the only way to get into them with out the password is to send it into the manufacture.

Freeride

RHCE, MCES(NT4,Win2000,Win2003), CNE, CCNA, VMWare VCP