

Re: NIS with local root

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2003-02/0004.html>

From: Kevin Jackson (kevin.jackson@genaware.com)

Date: 01/31/03

Date: Fri, 31 Jan 2003 21:51:32 -0000 (GMT)
From: "Kevin Jackson" <kevin.jackson@genaware.com>
To: <focus-linux@securityfocus.com>

Its clear that Linux is used in all sorts of environments – trusted, untrusted – with people replying with their 0.02 (local currency) – making the original post to this thread somewhat lost amongst us agreeing to disagree!

What works for some people doesn't work for others. There is no right or wrong answer – but one that just fits better.

For securing "lab users" that seem to be touted in these posts is quite different than someone trying to administer networked PCs in an office environment – where access to root isn't needed on a day-to-day basis and so mechanisms are put in place to disallow normal su'ing, or even logging on directly as root without some other bit of intervention first (say, deny root on the console and denying/removing su, but allowing access remotely from trusted administrator's PC).

We can argue for days on what is best for one environment – but others will find it either too restricting or unworkable.

If there is a utopian environment where networked file systems and remote security can be achieved and controlled then let the list know! I apologise, someone did suggest LDAP and some other form of remote file system. If we don't know about these alternatives, or they aren't well documented then this needs to be addressed.

Else, we'll be replying to the post below, ending up saying the person should have no input into the computer that has been turned off and shut in a room with no doors or windows.

In some cases that is a "utopian environment".

It would certainly make my job easier. :)

Kev

> *No, if someone has physical access to a PC they can turn it off,*
> *open the case, short the jumper to clear the BIOS, boot from a*

SecurityFocus Linux: Re: NIS with local root

- > floppy or CD and get root. Securing the services and network won't
- > help if you allow untrusted users to have unsupervised access [which is
- > eventually going to happen at some point in any classroom or lab] to
- > the hardware.

--

Kevin Jackson
Systems Administrator
GenaWare Limited

Locate, Enquire, Empower
www.genaware.com

PRIVILEGED - PRIVATE AND CONFIDENTIAL

This email and any files transmitted with it are intended solely for the use of the addressee(s) and may contain information which is confidential or privileged. If you receive this email and you are not the addressee (or responsible for delivery of the email to the addressee), please disregard the contents of the email, delete the email and notify the author immediately.

Before opening or using any attachments, please scan them for viruses and defects. We do not accept any liability for loss or damage, which may arise from your receipt of this e-mail. Our liability is limited to re-supplying any affected attachments.