

Re: root shell auditing

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2008-08/msg00010.html>

- *From:* security <security@xxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 06 Aug 2008 13:23:15 -0500
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

You can implement a simple system by using /usr/bin/script utility and pipe it a fifo on a NFS share for example. You need to establish a policy of course because there's an easy way to go around it. For more info and example read "man script".

Hope this helps,

Konstantin Ivanov

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.9 (MingW32)

Comment: Using GnuPG with Mozilla - <http://enigmail.mozdev.org>

iEYEARECAAYFAkiZ6UUACgkQB3wRB5KUBPm7ngCgmcJBxNerBnxIA4DNsLYnvaWn
ofUAoIHiesDT9IAJKHQimkUkofUksSCP
=nJTI

-----END PGP SIGNATURE-----

Hari Sekhon wrote:

Philip Turner wrote:

On 31 Jul 2008 at 10:24, Hari Sekhon wrote:

Diego
Lacerda
wrote:

Re: root shell auditing

Hi,
Mars,

I
think
that
you
could
use
Linux
Process
Accounting
to
audit
everything
that
you
need
in
a
shell
environment.

I've tried
this, it lacks
some detail
if I
remember
correctly it

doesn't log params as it was designed for process accounting, not security auditing, which could mean missing a lot as sometimes it's the parameters that make all the difference between a normal and a dangerous action.

I'll just play play devil's advocate for a moment here, and suggest

Re: root shell auditing

Re: root shell auditing

that as you log more and more detail you increase the risk that you'll include sensitive information that shouldn't be revealed to whoever reviews the security logs. Eventually you've just replaced the need to trust the admins with the need to trust the security reviewers.

(I'm not saying you've reached this point yet, just that it's

something to think about each time you up the level of detail.)

Anyone would think I'm an evil security guy or something... ;-)

Seriously though, you're making an assumption that it's just admins.

Developers use the command line too and often aren't anywhere near as smart or industry educated as they think they are which is why sometimes it's very handy if you can check on what they've done.

A good example was a guy we had who was supposed to be a very good

developer but got a command wrong and stopped a website from working. I had his command in the logs and proved it was his fault. So much for being so smart.. you'd think someone who was so good would know how to use a simple command and not append "." and ".." as args which went outside the directory he intended to. If you make a mistake once, ok it's a typo, but he did the same thing the next day too so I had to tell him to be more careful, which I could since I had proof it was his fault (I had his cwd as well in this case to match against the relatives . and ..

Moral of the story: logging and auditing are very important and make me

feel much better.

-h