

Re: Strange command histories in hacked shell history

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-12/0046.html>

From: Dave (*mudman_at_metafocus.net*)

Date: 12/19/04

Date: Sat, 18 Dec 2004 17:35:35 -0800 (PST)

To: Craig Edwards <brain@winbot.co.uk>

> *You could change the permissions on the su binary, so that only users in the wheel group can even execute su. that way, when a non-wheel user attempts to su to a user in the wheel group, they simply get permission denied.*

This is a really good idea. I decided to try it as root and chmod gave me
chmod: su: Operation Not Permitted! The nerve! I'll have to have a look
at that more carefully later :)

As a side note, I think Bill's point about 2 passwords to break is pretty strong in my point of view. Just for simplicity's sake (in both security and in design), "the su stack" really shouldn't be any larger than 1. No su'ing twice, or N number of times. Hmm, I wonder if there is an option for setting that. I suppose someone might have a purpose to, but if they really need to be doing that, I think they have a problem in their own designs.

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"