

comp.security.ssh: Re: Public key authentication defeats passwd age warning.

Re: Public key authentication defeats passwd age warning.

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2004-08/0239.html>

From: The other Thomas Gardner (*tGARDNER_at_ElectEngrngCompSci.CaseWesResUniv.EDU*)
Date: 08/27/04

Date: 27 Aug 2004 16:48:24 GMT

Darren,

Thanks a bunch for getting back to me. I sure appreciate it. I was just about to send basically the same note to openssh-unix-dev, but I guess I don't have to now...

Darren Tucker <dtucker@dodgy.net.au> wrote:

- > *In OpenSSH's native password support, password expiry is only checked*
- > *during password authentication, and the warning is generated as part of*
- > *that check (auth_shadow_pwexpired in auth-shadow.c).*
- >
- > *In PAM's world view, password expiry is done as part of the account checks*
- > *(ie pam_acct_mgmt) which sshd must check for all auth types (since it*
- > *has no idea what criteria PAM might use for those checks).*

Good info, thanks. Confirms what I'd guessed would be the case.

- > *It would be possible to generate the messages for non-password auths too*
- > *but I'm not sure it makes sense. If you're not using the password at all,*
- > *is it relevant that it's expired?*

Yes, because my customer sez so. :-)

Seriously, though, the passwd expiration isn't to keep you out, it's meant to try to help limit the exposure to the unauthorized folks in case they manage to get your passwd some day. OK, so YOU never use the passwd, however, in a sensitive environment, it still makes sense to me that you'd still want to change it on a regular basis in the off chance that someone else got their hands on it and THEY are using it (even if you aren't). That's what passwd expiration (in general) is all about, no?

- > *And what do you do if it is? Deny the*
- > *login even though the credentials used for the authentication (ie the*
- > *public key) are perfectly fine? Or generate a message of the form "your*
- > *password expired X days ago"?*

Re: Public key authentication defeats passwd age warning.

comp.security.ssh: Re: Public key authentication defeats passwd age warning.

That part does actually work the ``right" (depending on your view of the world) way now. If I log in and my passwd has expired, but it's still before my account is disabled due to over-expired passwd, it prompts me to change my passwd. Just like if I were logging in any other way. If I don't get it changed between the time the passwd expires and the cutoff, it should then disallow access all together (haven't tested that part yet, though, but I suspect PAM is gonna handle that so that should probably work that way, yes?).

That really only covers the login case, however. I would imagine that for scp or when you do ``ssh machine command arg" type thing, I would think the right behavior should probably be to simply deny access (yes even with a perfectly valid key), since there's no guarantee that there will be anyone at the keyboard. I haven't tested that either, though. I spent most of my time trying to figger out why I wasn't getting my warnings. Whatever it currently does is probably fine, though. That's a topic for another day.

Thanks again for the reply. I sure do appreciate it. If you'd like to narrow down where I should look to try to figger out how to put those warnings in, I sure would appreciate it. I'm not at all familiar with this code. If I do figger it out, I'll send you a patch. If you decide you agree with that behavior, you can stick it in, if you don't, well, I'll just have my own version, I suppose (assuming I even *CAN* figger out what to do, of course).

On the other hand, if you know just what to do and wanna send ME a patch, I'd appreciate that even more! :-) I'm sure you could get it done a LOT sooner than I could (and you'd probably even do it right, too).

Thanks,
tg.

> --

> *Darren Tucker (dtucker at zip.com.au)*

> *GPG key 8FF4FA69 / D9A3 86E9 7EEE AF4B B2D4 37C9 C982 80C7 8FF4 FA69*

> *Good judgement comes with experience. Unfortunately, the experience*

> *usually comes from bad judgement.*

--

To reply by mail, remove all lower case letters in my return address (tGARDNER@ElectEngrngCompSci.CaseWesResUniv.EDU).