

Re: Public key authentication troubles

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2004-05/0247.html>

From: Nicolas Bertolotti (*nbertolo_at_chez.com*)

Date: 05/27/04

Date: Thu, 27 May 2004 00:46:09 +0200

Yes, but then, the owner of the .ssh folder and the .ssh/authorized_keys file would not be "victim" anymore and, as far as I remember, sshd wouldn't accept the key in this case.

"Mike Delaney" <mdelan@computer.org> a écrit dans le message de news:slrncb9vph.8qe.mdelan@shell.lusars.net...

> *On Wed, 26 May 2004 21:10:55 +0200 in*

> *<c92pom\$kn\$1@news-reader1.wanadoo.fr>*,

> *Nicolas Bertolotti said something similar to:*

> :

> *: Anyway, I still don't understand the reason why such a restriction exists*

> *: (even in strict mode). As long as the .ssh directory contents is protected,*

> *: it should not be possible for a group member to do something bad on it.*

Am I

> *: wrong ?*

>

> *Without the restriction prohibiting group-writable home directories, an*

> *attack like the following would be possible:*

>

> *% mv ~victim/.ssh ~victim/.ssh_orig*

> *% mkdir ~victim/.ssh*

> *% cp ~/.ssh/id_rsa ~victim/.ssh/authorized_keys*

> *% ssh victim@localhost*

>