

Re: two SSH compatibility scenarios: can it work?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2002-10/1974.html>

From: Nico Kadel-Garcia (nkadel@bellatlantic.net)

Date: 09/09/02

From: "Nico Kadel-Garcia" <nkadel@bellatlantic.net>

Date: Mon, 09 Sep 2002 05:36:12 GMT

"Alan Tu" <alantu@students.uiuc.edu> wrote in message
news:GcId9.16964\$m7.157709@vixen.cso.uiuc.edu...

> *Hi, I use a lot of computers, especially Linux, and its nice to be able to
> log in remotely, and securely. Thank you OpenSSH. However, I have two
> connection scenarios which I'm not sure will work.*

>

> *1. We are required to use SSH to log into the Engineering lab machines.*

The

> *server software displays this header upon telnet connection to port 22.*

> *SSH-1.99-OpenSSH_3.4p1*

>

> *My question is, can I make the server do public-key based authentication,
or*

> *must the sysadmin enable this explicitly? Right now the SSH2*

authentication

> *is password-based.*

It's the sys-admin's job, but it's probably already set up by default. Ask
politely, or try with a public key in ~/.ssh/authorized_keys.

> *2. I still use Windows on my notebook for application compatibility. The
> campus people told us to install a specific software for SSH compatibility
> with all campus servers. Going to help/about, I see:*

> *SSH Secure Shell*

> *Version: 3.1.0 (Build 235)*

> *Copyright 2000-2001 SSH Communications Security Corp.*

>

> *This version has connected with the campus servers via password. However,*

> *because its for students, something called PKI has been removed. I run a*

> *Linux server at home which I would like to log into. Its a Mandrake system*

> *running OpenSSH 3.4p1 (patched). Here, I do want to use public-key*

> *authentication, so I generated a DSA key on the remote system, copied the*

> *id_dsa.pub into authorized_keys, and then copied id_dsa[.pub] onto my*

> *Windows computer. When I tried to connect, however, this Windows SSH*

client

> *said it could not read the keys and defaulted to password authentication.*

comp.security.ssh: Re: two SSH compatibility scenarios: can it work?

Use a baseball bat on your Windows admins. Proceed directly to Putty, CygWin with OpenSSH, or any of the other freeware clients.

- > *My question is, are the key formats incompatible? Is there a key I can*
- > *generate that this Windows SSH client can import and use?*

Look for CygWin, which uses OpenSSH natively: save yourself a lot of time and grief in a lot of ways.

- *Next message:* : ["Re: ssh_init: Network error: Connection refused"](#)
- *Previous message:* : ["Re: pam_chroot vs. chroot-patches for sshd"](#)
- *In reply to:* [Alan Tu: "two SSH compatibility scenarios: can it work?"](#)
- *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)