

Re: Rhosts authentication with openssh 3.7

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-11/0210.html>

From: Nico Kadel-Garcia (nkadel_at_comcast.net)

Date: 11/23/03

Date: Sun, 23 Nov 2003 11:13:39 -0500

"Neil W Rickert" <rickert+nn@cs.niu.edu> wrote in message
news:bpmaop\$lbm\$1@husk.cso.niu.edu...
> ludovic.leclerc@col.bsf.alcatel.fr (*ludovic LECLERC*) writes:
>
> >> *Either:*
>
> >> *Make "ssh" setuid*
>
> >> *chown ssh root*
> >> *chmod u+s ssh*
>
> >> *or:*
>
> >> *set EnableSSHKeysign to "yes" in your ssh_config*
> >> *file. (And make sure that ssh-keysign is setuid).*
>
> > *Is there still a way with openssh 3.7 to have an authentication only*
> > *based on .rhosts file (without RSA, DSA keys or stuff like that) ?...*
>
> *I haven't tried it. This was only ever possible with protocol 1.*
>
> *Why would you want to allow something that insecure? Best is to*
> *use ".shosts", and not ".rhosts"*
>
> *The host based authentication that does work uses ".rhosts" or*
> *".shosts", and uses the host keys. You need not generate any*
> *personal keys.*

As I remember, you also have to list the SSH client's hostkeys in a
"known_hostkeys" file, either the user's or the server system's. But it's
been a while since I last tried this....