

Re: Problem setting up passwordless connection

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2004-04/0323.html>

From: Jack Moe (*mojorisin_at_bigmailbox.net*)

Date: 04/27/04

Date: 27 Apr 2004 09:43:51 -0700

couzteau@bitfaeule.net (couzteau) wrote in message
news:<9a29ba16.0404241117.600dfd3d@posting.google.com>...

> *Hello,*

>

> *I have a minimal network: One machine is connected to the internet and*

> *acts as a firewall and router for another machine.*

>

> *I want to be able to connect from both machines to the other via ssh*

> *without typing passwords because i want to copy files programmatically*

> *with rsync.*

>

> *I read the man page and sucessfully configured this it for my root*

> *account. but i had no success with my regular (non-root) username.*

>

> *On both machines I'm running MacOSX 10.3.3 with*

> *OpenSSH_3.6.1p1+CAN-2003-0693, SSH protocols 1.5/2.0, OpenSSL*

> *0x0090702f.*

>

> *I set up /etc/hosts.equiv with the romote machines name and thei*

> *ip-addresses as well, i.e:*

> *192.168.50.1*

> *dixon.local*

>

> *i created keys and copied them to authorized keys on my local and my*

> *remote machine:*

> *ssh-keygen -t dsa -f ~/.ssh/id_dsa*

> *cat ~/.ssh/id_dsa.pub | ssh user@dixon.local 'cat - >>*

> *~/.ssh/authorized_keys'*

> *cat ~/.ssh/id_dsa.pub >> ~/.ssh/authorized_keys*

>

> *I still get prompted for a password on:*

> *ssh myname@dixon.local*

>

> *what else do i need to do to get this to work with my regular users?*

> *running ssh verbosely yields the following output:*

>

> ...

> *debug1: Next authentication method: publickey*

comp.security.ssh: Re: Problem setting up passwordless connection

> *debug1: Trying private key: /Users/myUser/.ssh/identity*
> *debug1: Offering public key: /Users/myUser/.ssh/id_rsa*
> *debug1: Authentications that can continue:*
> *gssapi,publickey,password,keyboard-interactive*
> *... (the entire output is included at the bottom)*
>
> *So i see that the local machine tries to use the local*
>
> *Thank you for help*
>
> *jacques*
>
> -----
> *OpenSSH_3.6.1p1+CAN-2003-0693, SSH protocols 1.5/2.0, OpenSSL*
> *0x0090702f*
> *debug1: Reading configuration data /etc/ssh_config*
> *debug1: Rhosts Authentication disabled, originating port will not be*
> *trusted.*
> *debug1: Connecting to dixon.local [fe80:4::2e0:7dff:fedc:8a3d] port*
> *22.*
> *debug1: Connection established.*
> *debug1: identity file /Users/jochen/.ssh/identity type -1*
> *debug1: identity file /Users/jochen/.ssh/id_rsa type 1*
> *debug1: identity file /Users/jochen/.ssh/id_dsa type 2*
> *debug1: Remote protocol version 1.99, remote software version*
> *OpenSSH_3.6.1p1+CAN-2003-0693*
> *debug1: match: OpenSSH_3.6.1p1+CAN-2003-0693 pat OpenSSH**
> *debug1: Enabling compatibility mode for protocol 2.0*
> *debug1: Local version string SSH-2.0-OpenSSH_3.6.1p1+CAN-2003-0693*
> *debug1: An invalid name was supplied*
> *Hostname cannot be canonicalized*
>
> *debug1: An invalid name was supplied*
> *A parameter was malformed*
> *Validation error*
>
> *debug1: An invalid name was supplied*
> *Hostname cannot be canonicalized*
>
> *debug1: An invalid name was supplied*
> *A parameter was malformed*
> *Validation error*
>
> *debug1: SSH2_MSG_KEXINIT sent*
> *debug1: SSH2_MSG_KEXINIT received*
> *debug1: kex: server->client aes128-cbc hmac-md5 none*
> *debug1: kex: client->server aes128-cbc hmac-md5 none*
> *debug1: SSH2_MSG_KEX_DH_GEX_REQUEST sent*
> *debug1: expecting SSH2_MSG_KEX_DH_GEX_GROUP*
> *debug1: SSH2_MSG_KEX_DH_GEX_INIT sent*
> *debug1: expecting SSH2_MSG_KEX_DH_GEX_REPLY*

comp.security.ssh: Re: Problem setting up passwordless connection

```
> debug1: Host 'dixon.local' is known and matches the RSA host key.
> debug1: Found key in /Users/jochen/.ssh/known_hosts:1
> debug1: ssh_rsa_verify: signature correct
> debug1: SSH2_MSG_NEWKEYS sent
> debug1: expecting SSH2_MSG_NEWKEYS
> debug1: SSH2_MSG_NEWKEYS received
> debug1: SSH2_MSG_SERVICE_REQUEST sent
> debug1: SSH2_MSG_SERVICE_ACCEPT received
> debug1: Authentications that can continue:
> gssapi,publickey,password,keyboard-interactive
> debug1: Next authentication method: gssapi
> debug1: Server GSSAPI Error:
> Miscellaneous failure
> No such file or directory
>
>
> debug1: Authentications that can continue:
> gssapi,publickey,password,keyboard-interactive
> debug1: Authentications that can continue:
> gssapi,publickey,password,keyboard-interactive
> debug1: Next authentication method: publickey
> debug1: Trying private key: /Users/jochen/.ssh/identity
> debug1: Offering public key: /Users/jochen/.ssh/id_rsa
> debug1: Authentications that can continue:
> gssapi,publickey,password,keyboard-interactive
> debug1: Offering public key: /Users/jochen/.ssh/id_dsa
> debug1: Authentications that can continue:
> gssapi,publickey,password,keyboard-interactive
> debug1: Next authentication method: keyboard-interactive
> debug1: Authentications that can continue:
> gssapi,publickey,password,keyboard-interactive
> debug1: Next authentication method: password
> jochen@dixon.local's password:
```

Read <http://www.snailbook.com/faq/no-passphrase.auto.html>

Very good explanation on how to implement what you want to do.

Use 'pageant' as it is more secure than NULL passphrases. Otherwise, get rid of the '/etc/hosts.equiv' (which is used for "R" utilities 'rcpr|rsh|rlogin' anyway) any '.rhosts' files, and disable the "R" utilities (via PAM if MacOS supports it, or via the services in the equivalent of *NIX's '/etc/inetd.conf').

Jack Moe