

can't get passphrase auth with RH9 to RH 7.3

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-04/0237.html>

From: donno (yo_donno@attbi.com)

Date: 04/22/03

From: "donno" <yo_donno@attbi.com>

Date: Tue, 22 Apr 2003 17:53:05 GMT

Hi folks –

I'm new to ssh, but not to network, or linux.
I can't seem to get passphrase auth working from my main RedHat9 box to a RedHat 7.3 box. I've checked and double-checked files and settings, but still RSA and public-key auth fails, and prompts me for my username password on the destination box.

I've followed every tutorial and tip file I've found, with no success. Of course, I've "ssh-keygen" my public and private keys, and placed the public keys in ~/.ssh/authorized_keys2 file on the destination box.

Here's a level 1 verbose output of an attempt.
TIA for any help!

–Don

----- cut here -----

```
[dradick@GOOBER dradick]$ ssh -v dradick@chops2
OpenSSH_3.5p1, SSH protocols 1.5/2.0, OpenSSL 0x0090701f
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Applying options for *
debug1: Rhosts Authentication disabled, originating port will not be trusted.
debug1: ssh_connect: needpriv 0
debug1: Connecting to chops2 [192.168.1.10] port 22.
debug1: Connection established.
debug1: identity file /home/dradick/.ssh/id_rsa type 1
debug1: identity file /home/dradick/.ssh/id_dsa type 2
debug1: Remote protocol version 2.0, remote software version OpenSSH_3.1p1
debug1: match: OpenSSH_3.1p1 pat OpenSSH_2.*,OpenSSH_3.0*,OpenSSH_3.1*
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_3.5p1
debug1: SSH2_MSG_KEXINIT sent
```

comp.security.ssh: can't get passphrase auth with RH9 to RH 7.3

```
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: dh_gen_key: priv key bits set: 129/256
debug1: bits set: 1583/3191
debug1: SSH2_MSG_KEX_DH_GEX_INIT sent
debug1: expecting SSH2_MSG_KEX_DH_GEX_REPLY
debug1: Host 'chops2' is known and matches the RSA host key.
debug1: Found key in /home/dradick/.ssh/known_hosts:1
debug1: bits set: 1589/3191
debug1: ssh_rsa_verify: signature correct
debug1: kex_derive_keys
debug1: newkeys: mode 1
debug1: SSH2_MSG_NEWKEYS sent
debug1: waiting for SSH2_MSG_NEWKEYS
debug1: newkeys: mode 0
debug1: SSH2_MSG_NEWKEYS received
debug1: done: ssh_kex2.
debug1: send SSH2_MSG_SERVICE_REQUEST
debug1: service_accept: ssh-userauth
debug1: got SSH2_MSG_SERVICE_ACCEPT
```

Hello, and welcome to SSH on CHOPS2 !

Ka Plah!

```
debug1: authentications that can continue: publickey,password,keyboard-interactive
debug1: next auth method to try is publickey
debug1: try pubkey: /home/dradick/.ssh/id_rsa
debug1: authentications that can continue: publickey,password,keyboard-interactive
debug1: try pubkey: /home/dradick/.ssh/id_dsa
debug1: authentications that can continue: publickey,password,keyboard-interactive
debug1: next auth method to try is keyboard-interactive
debug1: authentications that can continue: publickey,password,keyboard-interactive
debug1: next auth method to try is password
dradick@chops2's password:
debug1: ssh-userauth2 successful: method password
```