

problem with publickey authentication

Source: http://www.derkeiler.com/Mailing-Lists/securityfocus/Secure_Shell/2006-10/msg00049.html

- *From:* Duane Winner <dwinner@xxxxxxxx>
 - *Date:* Fri, 20 Oct 2006 08:37:09 -0400
-

Hello,

I have a business client who is running a SSH Communications SSH Tectia Server on a Windows NT Server.

I need to connect to their server from dozens of FreeBSD servers in my organization using OpenSSH client, using publickey auth only.

During testing, after entering the passphrase for private key, I am being prompted for a password, which has never happened to me before when connecting openssh->openssh.

He claimed that he tested on his side, and was able to connect from a Linux client to his own Windows Tectia SSH box.

So I copied my private key to an old Linux box, and tried that -- it worked as he claimed.

Why does openssh client behave differently between Linux and FreeBSD?

Or is it an issue with the versions of OpenSSH, and something changed?

Is there an option I can pass on my FreeBSD box to get my OpenSSH client to work as it does on the Linux box?

FreeBSD Client (cannot connect to server):
FreeBSD 5.5-RELEASE-p8
OpenSSH_3.8.1p1 FreeBSD-20060930, OpenSSL 0.9.7e-p1 25 Oct 2004

Linux Client (can connect to server):
Red Hat Linux 7.2 2.96-118.7.2) Red Hat 2.4.9-e.27smp
OpenSSH_3.1p1, SSH protocols 1.5/2.0, OpenSSL 0x0090602f

Windows Server:
Remote protocol version 2.0, remote software version 3.2.9 SSH Secure Shell Windows NT Server

Command on both FreeBSD and Linux Clients (again, works on Linux, fails on FreeBSD):
sftp -vvv -o IdentityFile=.ssh/testuserkey testuser@xxxxxxxxxxxxxxx

problem with publickey authentication

Logging on Linux:

```
Enter passphrase for key '.ssh/testuserkey':
debug1: read PEM private key done: type RSA
debug3: sign_and_send_pubkey
debug2: we sent a publickey packet, wait for reply
debug1: ssh-userauth2 successful: method publickey
```

and then I'm in.

Logging on FreeBSD (notice that I never get a reply from the server as I do when connecting from the Linux box. Why is this?):

```
Enter passphrase for key '.ssh/testuserkey':
debug1: read PEM private key done: type RSA
debug3: sign_and_send_pubkey
debug2: we sent a publickey packet, wait for reply
debug1: Authentications that can continue:
debug3: start over, passed a different list publickey,keyboard-interactive
debug3: preferred publickey,keyboard-interactive
debug3: authmethod_lookup publickey
debug3: remaining preferred: keyboard-interactive
debug3: authmethod_is_enabled publickey
debug1: Next authentication method: publickey
debug2: we did not send a packet, disable method
debug3: authmethod_lookup keyboard-interactive
debug3: remaining preferred:
debug3: authmethod_is_enabled keyboard-interactive
debug1: Next authentication method: keyboard-interactive
debug2: userauth_kbdint
debug2: we sent a keyboard-interactive packet, wait for reply
debug1: Authentications that can continue:
debug3: userauth_kbdint: disable: no info_req_seen
debug2: we did not send a packet, disable method
debug1: No more authentication methods to try.
Permission denied ().
```

Thanks for any help with this that anybody can provide!

-DW