

openssh's sshd for windows. Do I need an autho file?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-02/0309.html>

From: S. Eng (ngse@yahoo.com)

Date: 02/25/03

From: ngse@yahoo.com (S. Eng)
Date: 25 Feb 2003 11:17:14 -0800

Hi

I installed sshd (openssh) on my machine under windows nt.

The service started fine.

However, I could not ssh into it from anywhere. Should i have an authorization file or copying files to somewhere? Even when I do "ssh -v localhost", it was not taking my password. Here is a debug file when I try to log in from a Linux box. I want to do rsa and password login, but it seems like I cannot get the password alone to work.

Help is much appreciated. Thanks in advance...

```
OpenSSH_3.1p1, SSH protocols 1.5/2.0, OpenSSL 0x0090602f
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Applying options for *
debug1: Rhosts Authentication disabled, originating port will not be
trusted.
debug1: restore_uid
debug1: ssh_connect: getuid 500 geteuid 0 anon 1
debug1: Connecting to 128.220.18.129 [128.220.18.129] port 22.
debug1: temporarily_use_uid: 500/500 (e=0)
debug1: restore_uid
debug1: temporarily_use_uid: 500/500 (e=0)
debug1: restore_uid
debug1: Connection established.
debug1: read PEM private key done: type DSA
debug1: read PEM private key done: type RSA
debug1: identity file /home/sng1/.ssh/identity type -1
debug1: identity file /home/sng1/.ssh/id_rsa type -1
debug1: identity file /home/sng1/.ssh/id_dsa type -1
debug1: Remote protocol version 2.0, remote software version
OpenSSH_3.5p1
debug1: match: OpenSSH_3.5p1 pat OpenSSH*
Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_3.1p1
debug1: SSH2_MSG_KEXINIT sent
```

comp.security.ssh: openssh's sshd for windows. Do I need an autho file?

```
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: 134/256
debug1: bits set: 1602/3191
debug1: SSH2_MSG_KEX_DH_GEX_INIT sent
debug1: expecting SSH2_MSG_KEX_DH_GEX_REPLY
debug1: Host '128.220.18.129' is known and matches the RSA host key.
debug1: Found key in /home/sng1/.ssh/known_hosts:1
debug1: bits set: 1605/3191
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
```

****USAGE WARNING****

This is a private computer system. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized use. This computer system may be monitored for all lawful purposes, including to ensure that its use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored.

Use of this computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal

openssh's sshd for windows. Do I need an autho file?

comp.security.ssh: openssh's sshd for windows. Do I need an autho file?

prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

```
debug1: authentications that can continue:
publickey,password,keyboard-interactive
debug1: next auth method to try is publickey
debug1: try privkey: /home/sng1/.ssh/identity
debug1: try privkey: /home/sng1/.ssh/id_rsa
debug1: try privkey: /home/sng1/.ssh/id_dsa
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
sng1@128.220.18.129's password:
debug1: packet_send2: adding 48 (len 75 padlen 5 extra_pad 64)
Connection closed by 128.220.18.129
debug1: Calling cleanup 0x80634c0(0x0)
[1:59pm] [/home/sng1/.ssh]
```