

Re: ssh as non-root user

Source: http://www.derkeiler.com/Mailing-Lists/securityfocus/Secure_Shell/2006-07/msg00031.html

- *From:* "Nathan Jackson-Eeles" <c.cured@xxxxxxxx>
 - *Date:* Mon, 24 Jul 2006 11:24:02 +0200
-

Jonathan,

Don't know whether you fixed this or not, but I've just got round to reading this post.

The server is reporting the following to the client:
debug: server offers auth methods ".

I would check the syntax of your AllowedAuthentications in your sshd2_config.

I'm not sure whether it's just a typo in your mail, but it should begin with a capital "A":

AllowedAuthentications publickey

HTH,

Nathan

On 5/30/06, Jonathan Burelbach <jburelbach@xxxxxxx> wrote:

I am trying to setup sshd to run as a non-root user to limit connections to and from certain hosts. I'm running ssh.com v3.2.9 on Solaris 9 on an e25k and I am able to start sshd as myself, but login using keys doesn't work. I've got "allowedAuthentications" set to just "publickey" since passwd won't work and authorization and identification files are correct since I can login remotely using keys. Any one have any clues?

TIA.

The daemon tells me:

```
jburelba@barcelona: ~ 323 -> /usr/local/sbin/sshd -v
debug[23292]: SshConfig/sshconfig.c:2838: Metaconfig parsing stopped at line 3.
debug[23292]: SshConfig/sshconfig.c:3130: Read 10 params from config file.
sshd: SSH Secure Shell 3.2.9 on sparc-sun-solaris2.9
debug[23292]: SshHostKeyIO/sshhostkeyio.c:194: Reading public host key from
```

Re: ssh as non-root user

```
/export/home/jburelba/.ssh2/hostkey.pub
debug[23292]: SshHostKeyIO/sshhostkeyio.c:279: Host key algorithms (from disk): ssh-dss
debug[23292]: Becoming server.
debug[23292]: Creating listener
debug[23292]: Listener created
debug[23292]: no udp listener created.
debug[23292]: Running event loop
debug[23292]: Sshd2/sshd2.c:2007: new_connection_callback
debug[23292]: Sshd2/sshd2.c:1934: Wrapping stream with ssh_server_wrap...
debug[23292]: ssh_server_wrap: creating transport protocol
debug[23292]: Ssh2Transport/trcommon.c:3676: My version: SSH-2.0-3.2.9 SSH Secure
Shell
debug[23292]: ssh_server_wrap: creating userauth protocol
debug[23292]: Ssh2Common/sshcommon.c:537: local ip = 127.0.0.1, local port = 2022
debug[23292]: Ssh2Common/sshcommon.c:539: remote ip = 127.0.0.1, remote port = 58829
debug[23292]: SshConnection/sshconn.c:1945: Wrapping...
debug[23292]: Sshd2/sshd2.c:1972: done.
debug[23292]: new_connection_callback returning
debug[23292]: Remote version: SSH-1.99-3.2.9 SSH Secure Shell
debug[23292]: Major: 3 Minor: 2 Revision: 9
debug[23292]: Ssh2Transport/trcommon.c:1367: lang s to c: `', lang c to s: ``
debug[23292]: Ssh2Transport/trcommon.c:1433: c_to_s: cipher aes128-cbc, mac hmac-sha1,
compression none
debug[23292]: Ssh2Transport/trcommon.c:1436: s_to_c: cipher aes128-cbc, mac hmac-sha1,
compression none
debug[23292]: SshUnixUser/sshunixuser.c:408: Can't find jburelba's shadow - access denied.
debug[23292]: Sshd2/sshd2.c:1142: user 'jburelba' service 'ssh-connection' client_ip
'127.0.0.1' client_port '58829' completed "
debug[23292]: Sshd2/sshd2.c:1195: Number of groups: 2.
debug[23292]: Sshd2/sshd2.c:1200: Adding group: eos, 100.
debug[23292]: Sshd2/sshd2.c:1200: Adding group: sysadmin, 14.
debug[23292]: Sshd2/sshd2.c:1572: output: publickey
debug[23292]: Ssh2AuthCommonServer/auths-common.c:414: User jburelba's login is not
allowed due to system policy
debug[23292]: Ssh2AuthCommonServer/auths-common.c:41: publickey authentication
failed. Login to account jburelba not allowed or account non-existent.
debug[23292]: Sshd2/sshd2.c:1142: user 'jburelba' service 'ssh-connection' client_ip
'127.0.0.1' client_port '58829' completed "
debug[23292]: Sshd2/sshd2.c:1572: output:
debug[23292]: Ssh2Common/sshcommon.c:169: DISCONNECT received: No further
authentication methods available.
debug[23292]: Sshd2/sshd2.c:366: locally_generated = FALSE
debug[23292]: Ssh2Common/sshcommon.c:662: Destroying SshCommon object.
debug[23292]: SshConnection/sshconn.c:1997: Destroying SshConn object.
```

And the client says:

```
jburelba@barcelona: ~ 341 -> /usr/local/bin/ssh -v localhost -p 2022
debug: SshConfig/sshconfig.c:2838: Metaconfig parsing stopped at line 3.
debug: SshConfig/sshconfig.c:3130: Read 0 params from config file.
```

Re: ssh as non-root user

```
debug: Ssh2/ssh2.c:1707: User config file not found, using defaults. (Looked for
'/export/home/jburelba/.ssh2/ssh2_config')
debug: Connecting to localhost, port 2022... (SOCKS not used)
debug: Ssh2Transport/trcommon.c:3676: My version: SSH-1.99-3.2.9 SSH Secure Shell
debug: client supports 3 auth methods: 'publickey,keyboard-interactive,password'
debug: Ssh2Common/sshcommon.c:537: local ip = 127.0.0.1, local port = 58829
debug: Ssh2Common/sshcommon.c:539: remote ip = 127.0.0.1, remote port = 2022
debug: SshConnection/sshconn.c:1945: Wrapping...
debug: SshReadLine/sshreadline.c:2427: Initializing ReadLine...
debug: Remote version: SSH-2.0-3.2.9 SSH Secure Shell
debug: Major: 3 Minor: 2 Revision: 9
debug: Ssh2Transport/trcommon.c:1367: lang s to c: `', lang c to s: ``
debug: Ssh2Transport/trcommon.c:1433: c_to_s: cipher aes128-cbc, mac hmac-sha1,
compression none
debug: Ssh2Transport/trcommon.c:1436: s_to_c: cipher aes128-cbc, mac hmac-sha1,
compression none
debug: SshKeyFile/sshkeyfile.c:373: file
/export/home/jburelba/.ssh2/hostkeys/key_2022_localhost.pub does not exist.
debug: SshKeyFile/sshkeyfile.c:373: file /etc/ssh2/hostkeys/key_2022_localhost.pub does not
exist.
Host key not found from database.
Key fingerprint:
xuzil-vunov-migug-becur-kehib-zyfob-zedyn-kemeg-kahor-sysyf-muxux
You can get a public key's fingerprint by running
% ssh-keygen -F publickey.pub
on the keyfile.
Are you sure you want to continue connecting (yes/no)? yes
Host key saved to /export/home/jburelba/.ssh2/hostkeys/key_2022_localhost.pub
host key for localhost, accepted by jburelba Tue May 30 2006 14:53:05 -0500
debug: Ssh2Common/sshcommon.c:332: Received SSH_CROSS_STARTUP packet from
connection protocol.
debug: Ssh2Common/sshcommon.c:382: Received SSH_CROSS_ALGORITHMS packet
from connection protocol.
WARNING ** WARNING ** WARNING ** WARNING ** WARNING

This is a U.S. Government computer system, which may be accessed and used
only for authorized Government business by authorized personnel.
Unauthorized access or use of this computer system may subject violators to
criminal, civil, and/or administrative action. All information on this
computer system may be intercepted, recorded, read, copied, and disclosed by
and to authorized personnel for official purposes, including criminal
investigations. Such information includes sensitive data encrypted to comply
with confidentiality and privacy requirements. Access or use of this computer
system by any person, whether authorized or unauthorized, constitutes consent
to these terms. There is no right of privacy in this system.

WARNING ** WARNING ** WARNING ** WARNING ** WARNING

debug: server offers auth methods 'publickey'.
debug: Ssh2AuthPubKeyClient/authc-pubkey.c:1794: Starting pubkey auth...
```

Re: ssh as non-root user

```
debug: Ssh2AuthPubKeyClient/authc-pubkey.c:1739: Agent is running, asking keys...
debug: Ssh2AuthPubKeyClient/authc-pubkey.c:1549: Got 3 keys from the agent.
debug: Ssh2AuthPubKeyClient/authc-pubkey.c:1666: adding keyfile
"/export/home/jburelba/.ssh2/id_dsa_1024_b" to candidates
debug: Ssh2AuthPubKeyClient/authc-pubkey.c:1666: adding keyfile
"/export/home/jburelba/.ssh2/id_rsa_2048_a" to candidates
debug: Ssh2AuthPubKeyClient/authc-pubkey.c:1666: adding keyfile
"/export/home/jburelba/.ssh2/id_dsa_2048_a" to candidates
debug: Ssh2AuthPubKeyClient/authc-pubkey.c:1529: Trying 6 key candidates.
debug: server offers auth methods ".
debug: Ssh2Common/sshcommon.c:169: DISCONNECT received: No further authentication
methods available.
debug: SshReadLine/sshreadline.c:2485: Uninitializing ReadLine...
warning: Authentication failed.
Disconnected; no more authentication methods available (No further authentication methods
available.).
debug: Ssh2Common/sshcommon.c:662: Destroying SshCommon object.
debug: SshConnection/sshconn.c:1997: Destroying SshConn object.
Exit 78
```

--

```
=====+=====+=====+=====+=====+=====+=====+
Jonathan Burelba jburelba@xxxxxxxxxxxx
Unix Systems Administrator jburelba@xxxxxxx
NIH/CIT/DCSS/SOSB;12 South Dr.;Bldg 12B/2N207;Bethesda (301) 496-7372
```