

sftp from UNIX to Windows

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2005-04/0223.html>

gavinharris.home_at_gmail.com

Date: 04/25/05

Date: 25 Apr 2005 05:10:29 -0700

Hi All,

I have had a look through the groups for some information on this. Basically we have OpenSSH server running on the Windows box. I need to script a file transfer from the UNIX box to the Windows box.

I have got my head around using ssh-keygen, and have created a public / private key pair on the UNIX box. I have transferred the Public key to the Windows box and in the home directory created a .ssh folder and created an authorized_keys file. I here I copied in the contents of the public key. Try to log in using ssh -vvv ... and this is what I get:

---SNIP---

```
batchopr:/cust/home/batchopr/.ssh >ssh -vvv -i mykey
dev0066@m0180ukdox1
OpenSSH_3.7.1p2, SSH protocols 1.5/2.0, OpenSSL 0.9.7c 30 Sep 2003
debug1: Reading configuration data /var/nc/ssh/ssh_config
debug3: RNG is ready, skipping seeding
debug2: ssh_connect: needpriv 0
debug1: Connecting to m0180ukdox1 [10.33.10.102] port 22.
debug1: Connection established.
debug3: Not a RSA1 key file mykey.
debug2: key_type_from_name: unknown key type '-----BEGIN'
debug3: key_read: missing keytype
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
```

comp.security.ssh: sftp from UNIX to Windows

```
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug3: key_read: missing whitespace
debug2: key_type_from_name: unknown key type '-----END'
debug3: key_read: missing keytype
debug1: identity file mykey type 2
debug1: Remote protocol version 2.0, remote software version
OpenSSH_3.8.1p1
debug1: match: OpenSSH_3.8.1p1 pat OpenSSH*
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_3.7.1p2
debug3: RNG is ready, skipping seeding
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug2: kex_parse_kexinit:
diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
debug2: kex_parse_kexinit: ssh-rsa,ssh-dss
debug2: kex_parse_kexinit:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc
,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
debug2: kex_parse_kexinit:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc
,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
debug2: kex_parse_kexinit:
hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,
hmac-md5-96
debug2: kex_parse_kexinit:
hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,
hmac-md5-96
debug2: kex_parse_kexinit: none,zlib
debug2: kex_parse_kexinit: none,zlib
debug2: kex_parse_kexinit:
debug2: kex_parse_kexinit:
debug2: kex_parse_kexinit: first_kex_follows 0
debug2: kex_parse_kexinit: reserved 0
debug2: kex_parse_kexinit:
diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
debug2: kex_parse_kexinit: ssh-rsa,ssh-dss
debug2: kex_parse_kexinit:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc
,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
debug2: kex_parse_kexinit:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc
,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
debug2: kex_parse_kexinit:
hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,
hmac-md5-96
debug2: kex_parse_kexinit:
hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,
```

```
hmac-md5-96
debug2: kex_parse_kexinit: none,zlib
debug2: kex_parse_kexinit: none,zlib
debug2: kex_parse_kexinit:
debug2: kex_parse_kexinit:
debug2: kex_parse_kexinit: first_kex_follows 0
debug2: kex_parse_kexinit: reserved 0
debug2: mac_init: found hmac-md5
debug1: kex: server->client aes128-cbc hmac-md5 none
debug2: mac_init: found hmac-md5
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
debug2: dh_gen_key: priv key bits set: 127/256
debug2: bits set: 1063/2048
debug1: SSH2_MSG_KEX_DH_GEX_INIT sent
debug1: expecting SSH2_MSG_KEX_DH_GEX_REPLY
debug3: check_host_in_hostfile: filename
/cust/home/batchopr/.ssh/known_hosts
debug3: check_host_in_hostfile: match line 1
debug3: check_host_in_hostfile: filename
/cust/home/batchopr/.ssh/known_hosts
debug3: check_host_in_hostfile: match line 1
debug1: Host 'm0180ukdox1' is known and matches the RSA host key.
debug1: Found key in /cust/home/batchopr/.ssh/known_hosts:1
debug2: bits set: 1047/2048
debug1: ssh_rsa_verify: signature correct
debug2: kex_derive_keys
debug2: set_newkeys: mode 1
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug2: set_newkeys: mode 0
debug1: SSH2_MSG_NEWKEYS received
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug2: service_accept: ssh-userauth
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug2: key: mykey (106838)
debug1: Authentications that can continue:
publickey,password,keyboard-interactive
debug3: start over, passed a different list
publickey,password,keyboard-interactive
debug3: preferred publickey,keyboard-interactive,password
debug3: authmethod_lookup publickey
debug3: remaining preferred: keyboard-interactive,password
debug3: authmethod_is_enabled publickey
debug1: Next authentication method: publickey
debug1: Offering public key: mykey
debug3: send_pubkey_test
debug2: we sent a publickey packet, wait for reply
debug1: Authentications that can continue:
publickey,password,keyboard-interactive
```

comp.security.ssh: sftp from UNIX to Windows

```
debug2: we did not send a packet, disable method
debug3: authmethod_lookup keyboard-interactive
debug3: remaining preferred: password
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:
publickey,password,keyboard-interactive
debug3: userauth_kbdint: disable: no info_req_seen
debug2: we did not send a packet, disable method
debug3: authmethod_lookup password
debug3: remaining preferred:
debug3: authmethod_is_enabled password
debug1: Next authentication method: password
dev0066@m0180ukdox1's password:
```

---END SNIP---

I am struggling to work this one out.

Thanks for any help you can provide!