Subject: Re: Problem with X11 and VNC
Posted by slonghurst on Tue, 05 Sep 2006 09:06:41 GMT
View Forum Message <> Reply to Message

sorry here you go

$ ssh -X -vvv root@192.168.0.206
OpenSSH_4.3p2, OpenSSL 0.9.8b 04 May 2006
debug2: ssh_connect: needpriv 0
debug1: Connecting to 192.168.0.206 [192.168.0.206] port 22.
debug1: Connection established.
debug1: identity file /home/shaun/.ssh/identity type -1
debug1: identity file /home/shaun/.ssh/id_rsa type -1
debug1: identity file /home/shaun/.ssh/id_dsa type -1
debug1: Remote protocol version 1.99, remote software version OpenSSH_3.9p1
debug1: match: OpenSSH_3.9p1 pat OpenSSH_3.*
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_4.3
debug2: fd 3 setting O_NONBLOCK
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug2: kex_parse_kexinit: diffie-hellman-group-exchange-sha1,diffie-hellman-gro
up14-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,arcfour1
28,arcfour256,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-c
tr,aes192-ctr,aes256-ctr
debug2: kex_parse_kexinit: aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour1
28,arcfour256,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-c
tr,aes192-ctr,aes256-ctr
debug2: kex_parse_kexinit: hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@open
ssh.com,hmac-sha1-96,hmac-md5-96
debug2: kex_parse_kexinit: hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@open
ssh.com,hmac-sha1-96,hmac-md5-96
debug2: kex_parse_kexinit: none,zlib@openssh.com,zlib
debug2: kex_parse_kexinit: none,zlib@openssh.com,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-gro
up14-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-c
tr
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-c

tr
debug2: kex_parse_kexinit: hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@open
ssh.com,hmac-sha1-96,hmac-md5-96
debug2: kex_parse_kexinit: hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@open
ssh.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(1024<1024<8192) sent
debug1: expecting SSH2_MSG_KEX_DH_GEX_GROUP
debug2: dh_gen_key: priv key bits set: 131/256
debug2: bits set: 524/1024
debug1: SSH2_MSG_KEX_DH_GEX_INIT sent
debug1: expecting SSH2_MSG_KEX_DH_GEX_REPLY
debug3: check_host_in_hostfile: filename /home/shaun/.ssh/known_hosts
debug3: check_host_in_hostfile: match line 1
debug1: Host '192.168.0.206' is known and matches the RSA host key.
debug1: Found key in /home/shaun/.ssh/known_hosts:1
debug2: bits set: 510/1024
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: /home/shaun/.ssh/identity (0x0)
debug2: key: /home/shaun/.ssh/id_rsa (0x0)
debug2: key: /home/shaun/.ssh/id_dsa (0x0)
debug1: Authentications that can continue: publickey,gssapi-with-mic,password
debug3: start over, passed a different list publickey,gssapi-with-mic,password
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: Trying private key: /home/shaun/.ssh/identity
debug3: no such identity: /home/shaun/.ssh/identity

debug1: Trying private key: /home/shaun/.ssh/id_rsa
debug3: no such identity: /home/shaun/.ssh/id_rsa
debug1: Trying private key: /home/shaun/.ssh/id_dsa
debug3: no such identity: /home/shaun/.ssh/id_dsa
debug2: we did not send a packet, disable method
debug3: authmethod_lookup password
debug3: remaining preferred: ,password
debug3: authmethod_is_enabled password
debug1: Next authentication method: password
root@192.168.0.206's password:
debug3: packet_send2: adding 64 (len 55 padlen 9 extra_pad 64)
debug2: we sent a password packet, wait for reply
debug1: Authentication succeeded (password).
debug1: channel 0: new [client-session]
debug3: ssh_session2_open: channel_new: 0
debug2: channel 0: send open
debug1: Entering interactive session.
debug2: callback start
debug2: x11_get_proto: /usr/X11R6/bin/xauth -f /tmp/ssh-H7yp2Yo0K9/xauthfile gen
erate :0.0 MIT-MAGIC-COOKIE-1 untrusted timeout 1200 2>/dev/null
debug2: x11_get_proto: /usr/X11R6/bin/xauth -f /tmp/ssh-H7yp2Yo0K9/xauthfile lis
t :0.0 2>/dev/null
debug1: Requesting X11 forwarding with authentication spoofing.
debug2: channel 0: request x11-req confirm 0
debug2: client_session2_setup: id 0
debug2: channel 0: request pty-req confirm 0
debug3: tty_make_modes: ospeed 38400
debug3: tty_make_modes: ispeed 38400
debug3: tty_make_modes: 1 3
debug3: tty_make_modes: 2 28
debug3: tty_make_modes: 3 8
debug3: tty_make_modes: 4 21
debug3: tty_make_modes: 5 4
debug3: tty_make_modes: 6 0
debug3: tty_make_modes: 7 0
debug3: tty_make_modes: 8 17
debug3: tty_make_modes: 9 19
debug3: tty_make_modes: 10 26
debug3: tty_make_modes: 12 18
debug3: tty_make_modes: 13 23
debug3: tty_make_modes: 14 22
debug3: tty_make_modes: 18 15
debug3: tty_make_modes: 30 0
debug3: tty_make_modes: 31 0
debug3: tty_make_modes: 32 0
debug3: tty_make_modes: 33 0
debug3: tty_make_modes: 34 0
debug3: tty_make_modes: 35 0

debug3: tty_make_modes: 36 1
debug3: tty_make_modes: 37 0
debug3: tty_make_modes: 38 1
debug3: tty_make_modes: 39 0
debug3: tty_make_modes: 40 0
debug3: tty_make_modes: 41 0
debug3: tty_make_modes: 50 1
debug3: tty_make_modes: 51 1
debug3: tty_make_modes: 53 1
debug3: tty_make_modes: 54 1
debug3: tty_make_modes: 55 1
debug3: tty_make_modes: 56 0
debug3: tty_make_modes: 57 0
debug3: tty_make_modes: 58 0
debug3: tty_make_modes: 59 1
debug3: tty_make_modes: 60 1
debug3: tty_make_modes: 61 1
debug3: tty_make_modes: 70 1
debug3: tty_make_modes: 71 0
debug3: tty_make_modes: 72 1
debug3: tty_make_modes: 73 0
debug3: tty_make_modes: 74 0
debug3: tty_make_modes: 75 0
debug3: tty_make_modes: 90 1
debug3: tty_make_modes: 91 1
debug3: tty_make_modes: 92 0
debug3: tty_make_modes: 93 0
debug2: channel 0: request shell confirm 0
debug2: fd 3 setting TCP_NODELAY
debug2: callback done
debug2: channel 0: open confirm rwindow 0 rmax 32768
debug1: Remote: No xauth program; cannot forward with spoofing.
debug2: channel 0: rcvd adjust 131072
[root@aquarius ~]# debug2: client_check_window_change: changed
debug2: channel 0: request window-change confirm 0
debug2: client_check_window_change: changed
debug2: channel 0: request window-change confirm 0