

ssh2 hostbased auth in 3.4

Source: http://www.derkeiler.com/Mailing-Lists/securityfocus/Secure_Shell/2003-06/0127.html

From: Jackson, Jonah (jjackson_at_iknowmed.com)

Date: 06/18/03

Date: Tue, 17 Jun 2003 17:46:53 -0700

To: <seureshell@securityfocus.com>

I'm using the Redhat rpm for 3.4p1 and am right on the edge of getting hostbased auth to work, but I'm getting an error message that I'm not able to track down.

I've done the following

Server Side:

- created /etc/ssh/ssh_known_hosts and put added entry for client rsa public key.
- added entry for client in \$HOME/.shosts of user I want to enable hostbased auth for
- edited /etc/sshd_config:
 - HostbasedAuthentication yes
 - IgnoreRhosts no

Client Side

- enabled HostbasedAuthentication in /etc/ssh_config

Everything looks like it's working except at the very end, the server side reports the following:

```
debug3: monitor_read: checking request 22
mm_answer_keyverify: bad signature data blob
debug1: Calling cleanup 0x80549c0(0x0)
debug1: Calling cleanup 0x8071110(0x0)
debug1: Calling cleanup 0x8071110(0x0)
```

I've looked through this mailing list and the developer list and I can't find anything that refers to this particular error message. I know there are a bunch of threads on hostbased auth so I'm probably missing something very obvious here, but any help would be appreciated.

Thanks.

Jonah Jackson
Senior Network Engineer
iKnowMed
jjackson@iknowmed.com

Full Server Side Debug (you'll have to forgive me for the *replaced ip* and *replaced hostname* bits, but rest assured that they are the correct name and address):

SecurityFocus Secure Shell: ssh2 hostbased auth in 3.4

```
Connection from *replaced ip* port 38593
debug1: Client protocol version 2.0; client software version OpenSSH_3.4p1
debug1: match: OpenSSH_3.4p1 pat OpenSSH*
Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_3.4p1
debug2: Network child is on pid 18275
debug3: preauth child monitor started
debug3: mm_request_receive entering
debug3: privsep user:group 74:74
debug1: list_hostkey_types: ssh-rsa,ssh-dss
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
debug2: kex_parse_kexinit:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
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
```