

# SSH Debugging <-- compatibility

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2001-12/0276.html>

---

**From:** Bogomips ([bogomips....@nirvanet.net](mailto:bogomips....@nirvanet.net))

**Date:** 12/21/01

From: "Bogomips" <[bogomips....@nirvanet.net](mailto:bogomips....@nirvanet.net)>

Date: Fri, 21 Dec 2001 18:42:29 +0100

Well,

Just imagine a large production area with plenty of powerfull printers. The printers use NT file servers to keep spool. We use wireless connectivity and encryption is on the "off" mode for performance concerns. To keep info safe from Geeks, we are re-writting application to systematically use scp for file transferts.

Ok, well... We face this buggy situation....

```
[admin@host ]$ ssh -C -v -c twofish -l admin server
```

```
debug: Connecting to server, port 22...
```

```
debug: Ssh2/ssh2.c:1956/main: Entering event loop.
```

```
debug: Ssh2Client/sshclient.c:1330/ssh_client_wrap: Creating transport protocol.
```

```
debug:
```

```
SshAuthMethodClient/sshauthmethod.c:137/ssh_client_authentication_initialize: Added "publickey" to usable methods.
```

```
debug:
```

```
SshAuthMethodClient/sshauthmethod.c:137/ssh_client_authentication_initialize: Added "password" to usable methods.
```

```
debug: Ssh2Client/sshclient.c:1362/ssh_client_wrap: Creating userauth protocol.
```

```
debug: client supports 2 auth methods: 'publickey,password'
```

```
debug: Ssh2Common/sshcommon.c:496/ssh_common_wrap: local ip = 10.10.100.1, local port = 34791
```

```
debug: Ssh2Common/sshcommon.c:498/ssh_common_wrap: remote ip = 10.10.100.10, remote port = 22
```

```
debug: SshConnection/sshconn.c:1889/ssh_conn_wrap: Wrapping...
```

```
debug: Remote version: SSH-2.0-2.4.0 SSH Secure Shell Windows NT Server Evaluation (Expires Sun Jan 20 2002)
```

```
debug: Major: 2 Minor: 4 Revision: 0
```

```
1. debug: Ssh2Transport/trcommon.c:1286/ssh_tr_input_version: Remote version has kex packet guess determination bug.
```

```
2. debug: Ssh2Transport/trcommon.c:1290/ssh_tr_input_version: Remote version
```

has hostbased looping on failure bug.

line 1 & 2 repport a buggy situation. What does it mean?

debug: Ssh2Transport/trcommon.c:1294/ssh\_tr\_input\_version: Remote version can only handle one key in "hostbased" auth.

debug: Ssh2Transport/trcommon.c:1366/ssh\_tr\_input\_version: Remote version uses md5 instead of sha-1 as hash algorithm with RSA keys.

debug: Ssh2Transport/trcommon.c:1717/ssh\_tr\_negotiate: lang s to c: `', lang c to s: `'

3. debug: Ssh2Transport/trcommon.c:1783/ssh\_tr\_negotiate: c\_to\_s: cipher twofish-cbc, mac hmac-sha1, compression none

4. debug: Ssh2Transport/trcommon.c:1786/ssh\_tr\_negotiate: s\_to\_c: cipher twofish-cbc, mac hmac-sha1, compression none

compression none... Thus, my -C switch was not usefull...

debug: Remote host key found from database.

debug: Ssh2Common/sshcommon.c:291/ssh\_common\_special: Received SSH\_CROSS\_STARTUP packet from connection protocol.

debug: Ssh2Common/sshcommon.c:341/ssh\_common\_special: Received SSH\_CROSS\_ALGORITHMS packet from connection protocol.

This is an evaluation version of the SSH Secure Shell Windows Server.

The evaluation version expires on Sun Jan 20 2002)

debug: server offers auth methods 'password'.

debug: Ssh2AuthPasswdClient/authc-passwd.c:95/ssh\_client\_auth\_passwd:

Starting password query...

admin's password:

Compression is absolutely necessary because the wireless bandwidth is very low.

[admin@host]\$ ssh -V

ssh: SSH Secure Shell 3.0.1 (non-commercial version) on i686-pc-linux-gnu

At the NT side:

SSH Secure Shell for Windows Servers.

Any idea?

Regards,

Bogomips

- 
- **Next message:** [Roger: "SSH File Transfers"](#)
  - **Previous message:** [nickd@nospam.demon.co.uk: "Re: ssh and hosts.allow; purpose of ssh"](#)
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)