

<http://www.coincoin.fr.eu.org/?SSH-debugging-sucks>



SSH debugging sucks

- 6- Webographie -

Date de mise en ligne : jeudi 9 janvier 2014

Copyright © L'Imp'Rock Scénette (by @_daffyduke_) - Tous droits réservés

How much human productivity is lost every day due to the horrible debugging messages in SSH ? I bet it is thousands of hours world-wide. It isn't just sysadmins : programmers, web developers, and many non-technical users are frustrated by this.

I'm pretty good at debugging ssh authentication problems. The sad fact is that most of my methodology involves ignoring the debug messages and just "knowing" what to check. That's a sad state of affairs.

The debug messages for "ssh -v" should look like this :

```
HELLO! I AM TRYING TO LOG IN. I'VE TOLD THE SERVER I CAN USE (method,method,method). I AM NOW TRYING TO LOG
IN VIA (method). I AM SENDING (public key). THAT DID NOT WORK. I AM SAD. I AM NOW TRYING TO LOG IN VIA
(method). I AM SENDING USERNAME foo AND a password of length x. THAT DID WORK. I AM LOGGING IN. I AM
HAPPY.</code>
```

Similarly on the server side, "sshd -d" should look more like :

```
HELLO! SOMEONE HAS CONTACTED ME FROM IP ADDRESS 1.1.1.1. THEY HAVE TOLD ME THEY CAN LOG IN USING THE
FOLLOWING METHODS: (method1,method2,method3). THEY ARE NOW TRYING (method) THEY GAVE ME (first 100 bytes of
base64 of public key) THAT DID NOT WORK. TIME TO TRY THE NEXT METHOD. THEY ARE NOW TRYING (method) THEY GAVE
ME A PASSWORD OF LENGTH x THAT DID WORK. I WILL LET THEM LOG IN NOW.
```

Instead we have to look at messages like :

```
debug1: monitor_child_preauth: tal has been authenticated by privileged process debug3: mm_get_keystate:
Waiting for new keys debug3: mm_request_receive_expect entering: type 26 debug3: mm_request_receive entering
debug3: mm_newkeys_from_blob: 0x801410a80(150) debug2: mac_setup: found hmac-md5-etm@openssh.com debug3:
mm_get_keystate: Waiting for second key debug3: mm_newkeys_from_blob: 0x801410a80(150)ÿ
```

Sigh.

I actually started looking at the source code to OpenSSH today to see how difficult this would be. It doesn't look too difficult. Sadly I had to stop myself because I was procrastinating from the project I really needed to be working on.

I'd consider paying a "bounty" to someone that would submit a patch to OpenSSH that would make the debug logs dead simple to understand. Maybe a kickstarter would be a better idea.

The hard part would be deciding what the messages should be. I like the [Kibo-esque](#) (well, actually [B1FF-esque](#)) version above. I hope you do too.

If anyone is interested in working on this, I'd be glad to give input. If someone wants to do a kickstarter I promise to be the first to donate.

[EverythingSysadmin?d=yIl2AUoC8zA](#)
[EverythingSysadmin?i=02VP-mBR3q0:eAcpnz0](#) [EverythingSysadmin?d=7Q72WNTAKBA](#)
[EverythingSysadmin?d=qj6IDK7rITs](#) [EverythingSysadmin?d=l6gmwiTKsz0](#)
[EverythingSysadmin?i=02VP-mBR3q0:eAcpnz0](#)
[02VP-mBR3q0]

Cet article est repris du site <http://feeds.everythingsysadmin.com...>