

Re: Failed Password Error

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-12/0179.html>

From: Darren Tucker (*dtucker_at_dodgy.net.au*)

Date: 12/21/03

Date: Sun, 21 Dec 2003 07:35:07 +0000 (UTC)

In article <ie4auv0heg71m050alksqiu67n875vdcfp@4ax.com>, Mark Olbert <mark@arcabama.com> wrote:

>I'm afraid I'm a total loss when it comes to using gdb. When I try to
>follow your instructions, I can telnet to port 2022

Try "ssh -p 2022 yourserver"

>Yes, it's Linux 2.4.20.

Which distribution and version? Which modules in your sshd PAM stack?

>Which may explain why 3.6.1p1 works. I've seen references to
>keyboard-interactive authentication on the web, but I can't find an
>explanation of it in the docs.

Simplifying somewhat, ssh2 (and ssh1 for that matter) support multiple authentication schemes. Password authentication is a single exchange, where the username and password fields are fixed by the protocol, eg:
client -> server: password authentication, user=myname, password=mypass123
client <- server: authenticated=yes

whereas keyboard-interactive (aka ChallengeResponse, aka Generic Message Exchange Authentication) is an exchange of one or more (more or less) arbitrary messages, which collectively decide the success or otherwise of the authentication, eg:

```
client -> server: challenge-response authentication
client <- server: challenge="Password:"
client -> server: response="mypass123"
client <- server: challenge="Password expired, enter new one:"
client -> server: response="newpass78"
client <- server: challenge="Confirm new password:"
client -> server: response="newpass78"
client <- server: authenticated=yes
```

The old code (<3.7p1) worked by assuming that the first prompt from PAM was a password prompt and deciding the authentication entirely based on the result of that. This was true most of the time but need not be, which is why the code was changed.

comp.security.ssh: Re: Failed Password Error

For further info see:

<http://www.ietf.org/internet-drafts/draft-ietf-secsh-userauth-18.txt>

<http://www.ietf.org/internet-drafts/draft-ietf-secsh-auth-kbdinteract-05.txt>

*>Is it possible that my problem is just
>that I'm trying to do password authentication when I need to be doing
>keyboard-interactive, whatever that is?*

No, I don't think that's the problem (and if you set
PasswordAuthentication=no on the server then it won't offer it).
You can see which authentications are passed by using "ssh -v".

--

Darren Tucker (dtucker at zip.com.au)

GPG key 8FF4FA69 / D9A3 86E9 7EEE AF4B B2D4 37C9 C982 80C7 8FF4 FA69

Good judgement comes with experience. Unfortunately, the experience
usually comes from bad judgement.