

password policies

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.setup/2004-12/0830.html>

rob.pellicaan_at_sns.nl

Date: 12/29/04

Date: 29 Dec 2004 05:29:01 -0800

Hi,

I am trying to implement several password policies on SuSe Linux

- A user password must have a length of 8 characters
- All user passwords may not repeat more than 2 characters
- The rootuser password must contain at least 2 non-alphabetic characters
- A new chosen password must at least be unchangeable for 3 days
- A password must be changed within 60 days
- The last 12 chosen passwords cannot be reused
- Users must be warned 5 days before their password expires
- A useraccount is locked when 3 consecutive unsuccessful login attempts occur

Now ONLY the first items (password length) I could set (PASS_MIN_LEN 8 in /etc/login.defs)

But could anybody tell me how to set the other?

By default 'Cracklib' support is enabled (password: use_cracklib md5 nullok in /etc/pam.d/passwd).

OBSCURE_CHECKS_ENAB in the login.defs is also set to yes
But both options do not seem to help matters; when I for example try to set a password using only lowercase characters, say 'qwertyuiopasd' (of minimum password length), the system simply allows me without a warning.

I also tried to specify passwd to use pam_cracklib.so (in /etc/pam.d/passwd) instead of pam_pwcheck with the following parameters: retry=3 debug dcredit=-1 ucredit=-1 ocredit=-1 lcredit=-1 minlen=12.

Now the strange is that boh retry=3 and debug are working fine, but the other settings seem to be ignored on passwd. But even worse, with my new password set, I can't login with that new password. Is there a know bug in the cracklib module?

I am using Suse 8.2 out of the box.

What am I doing wrong?