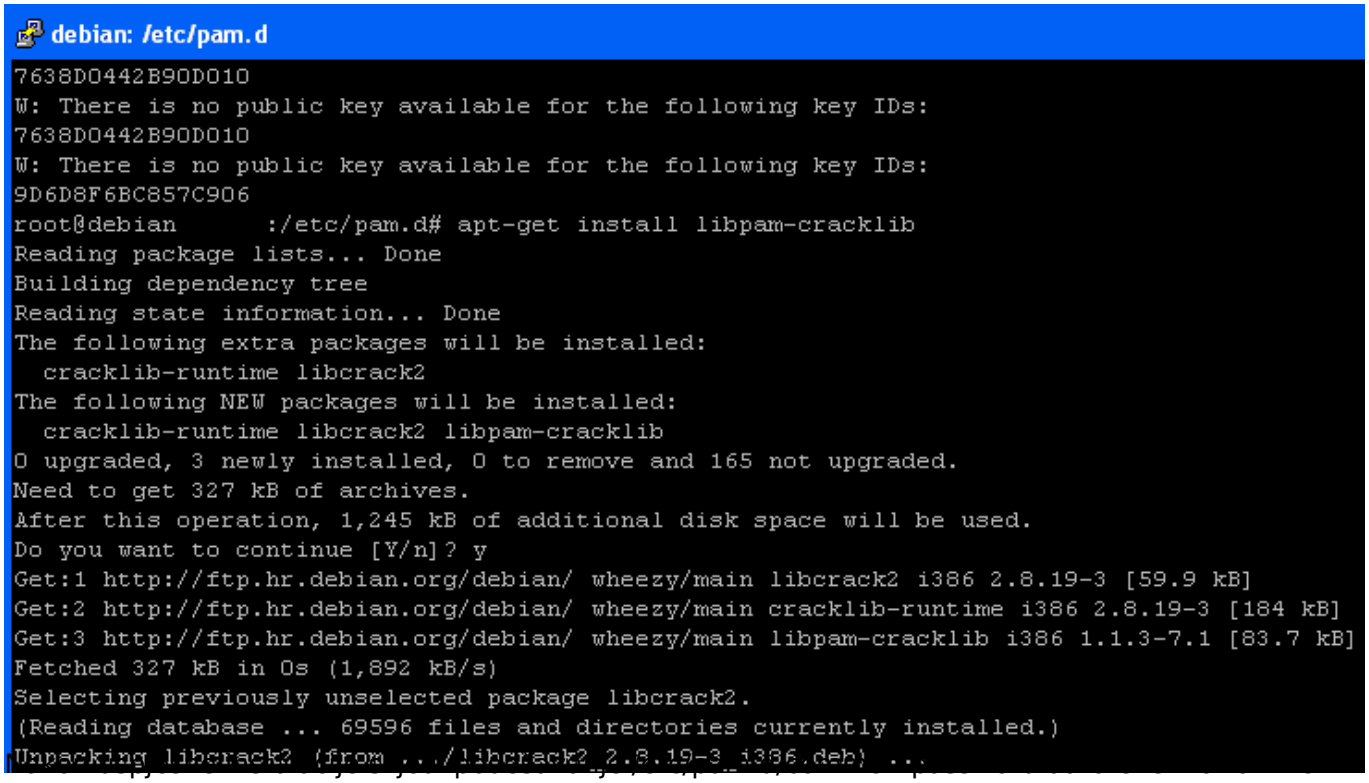
Zabrana korištenja stare zaporke

Naši korisnici uvijek traže što jednostavnije načine upotrebe resursa koji su im dodijeljeni, ne vole učiti i ne žele pamtiti previše stvari. Tako ne vole ni mijenjati zaporku (Čemu, kad je i stara zaporka dobra?). Vaš poslužitelj, iz sigurnosnih razloga, možete podesiti tako da korisniku nakon nekoliko mjeseci istekne zaporka, pa ga sustav prisiljava da je promjeni, ali korisnici kao korisnici, najčešće opet utipkaju staru zaporku.

No, postoji način kako onemogućiti recikliranje starih zaporki. Da bi korisnika prisilili da prilikom izmjene zaporke odabere posve novu zaporku, na sistemu moramo napraviti nekoliko jednostavnih izmjena u "pam" (Pluggable Authentication Modules) konfiguraciji za autentikaciju.

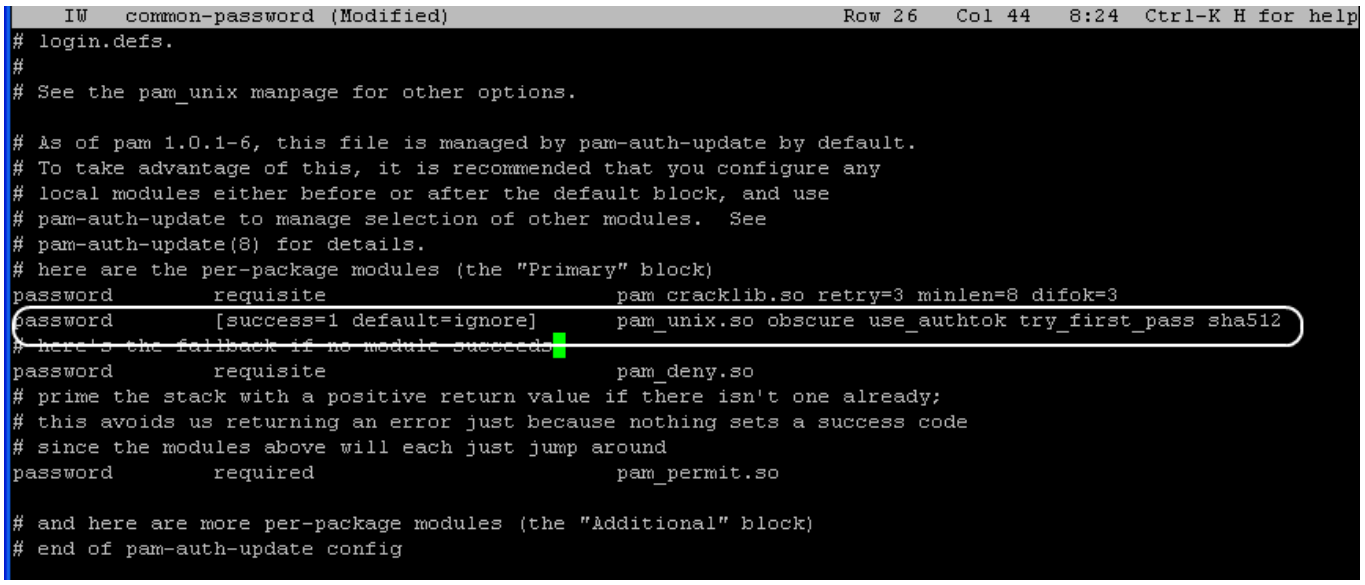
Prvi korak je instalacija "cracklib" modula koji se koristi za provjeru i usporedbu jakosti odabrane zaporke.

```
# apt-get update
# apt-get upgrade
# apt-get install libpam-cracklib
```



redak:

```
 password [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass s
ha512:
```

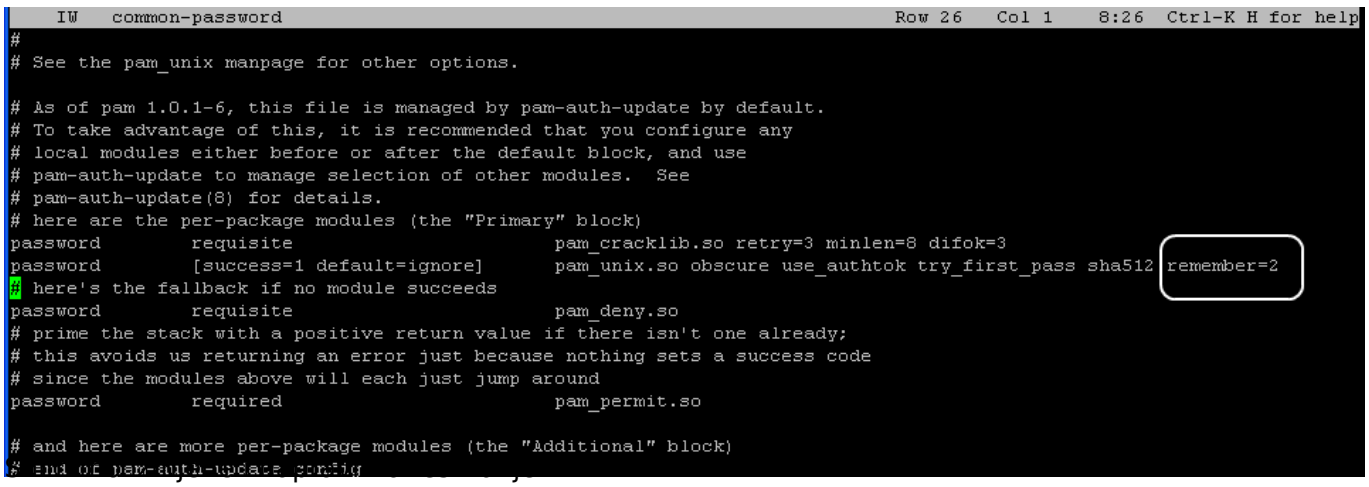


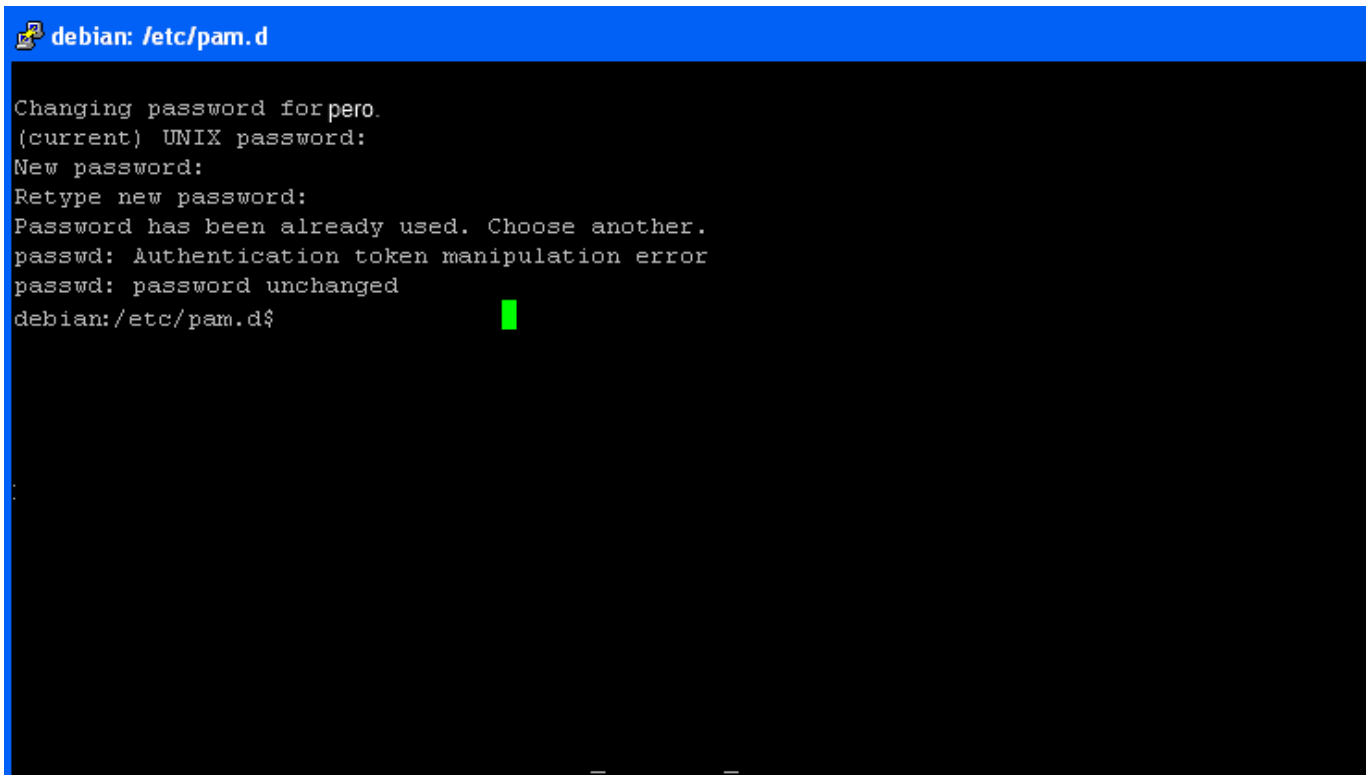
- **obscure** – uklju?uje dodatne provjere jakosti zaporke
- **use_authtok**
 – prisiljava modul da ne traži od korisnika novu zaporku, nego trenutnu
- **try_first_pass**
 – korisi se prva zaporka za sve module, u slu?aju da prva zaporka nije valjanja traži se nova
- **sha512 –** enkripcija

Na sam kraj linije, točnije iza enkripcije sha512, dodamo "**remember=broj**" gdje broj označava koliko dugo želimo čuvati stare zaporke.

Ako upišemo primjerice broj 2, sistem će čuvati zadnje dvije zaporke i neće dopustiti da se one ponove, ako upišemo 5 čuva zadnjih pet zaporki i tako dalje. Ovaj "povijesni" dio nalazi se u /etc/**oshadow** datoteci.

```
password [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass sha512 remember=2
```





Kao što se vidi iz primjera prilikom izmjene zaporke i pokušaja upisa iste kojom smo se prijavili dobijemo obavijest da je zaporka već bila korištena te da se odabere nova.

Ono što bi još trebalo postaviti je minimalna duljina zaporke. Ponovo editirajmo datoteku /etc/pam/common-passwd i pronađimo liniju passwd.

Tu upišemo "minlen=8", što govori da je minimalna duljina zaporke 8 znakova:

```
password requisite pam_cracklib.so retry=3 minlen=8
```

Još jedan primjer je prisiljavanje korisnika da prilikom promjene zaporke mora upisati minimalno 3 broja (da nisu svi znakovi slova):

password requisite pam_cracklib.so retry=3 minlen=8 dcredit=-2

dcredit – prisiljava unos brojeva

Naravno da možete uključiti i neke druge uvjete, poput uporabe velikih i malih slova te ostalih znakova.

U gornjoj liniji samo još dodajte:

ucredit=N – za unos velikih slova N – zeljeni broj
lcredit=N – za unos malih slova N – zeljeni broj
ocredit=N – za unos ostalih znakova

pet, 2016-04-15 09:13 - Zdravko Rašić**Kuharice:** Linux [1]
Kategorije: Sigurnost [2]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1634

Links
[1] https://sysportal.carnet.hr/taxonomy/term/17
[2] https://sysportal.carnet.hr/taxonomy/term/30