

The sys admin's daily grind: PWGen

CRYPTIC CODER

Easy to remember but still safe – this is the classic conflict when it comes to choosing a password. The PWGen tool offers a sensible compromise.

BY CHARLY KÜHNAST

If you recall, I complained about weak passwords in issue 84 [1]. The Fail2ban tool I talked about prevents disasters, but it really only treats the symptoms. If I choose the timing parameters carefully, Fail2ban will repel brute force attacks, but it stands no chance against password post-its on the keyboard or easily guessed passwords (Figure 1). As is always the case in security technology, the desired degree of protection determined by the admin and convenience, which is what users prefer, are in conflict.

Rotating the passwords every four weeks on top of other security requirements wears on users' patience; plus, you can't expect them to remember stuff like this. So your users write down their passwords and Murphy's Law dictates that they will leave their notes at the worst possible place. The opposite side of the coin is an environment in which the admin lets the users have their way

and end up with passwords like *tux* or *top_secret*. So what's your next move?

Password Distributor

PWGen [2] offers a compromise: The tool generates passwords with configurable properties. Calling PWGen without any parameters in the shell gives me a list of passwords with lower- and upper-case letters and numbers. *pwgen -s -y* gives you really robust passwords that might look something like this:

```
+3HEg,_5
1P.A@=2U
@||{}9Cy
```

But PWGen can generate simpler passwords without putting security on a level with your neighbor's dog's name. PWGen will not use non-standard characters by default, and the *-B* parameter suppresses characters that users tend to confuse, such as *l* and *I* or *O* and *0*. If you make a concession and do without

```
File Edit View Terminal Tabs Help
charly@salami:~$ pwgen -0
Feixeeng pohgaYah uMieecogh phieChip ideiSeil loaNapie Nouwenah doShiuta
Eipoonej Uyaijeng kokahLah Pheweepo auGhaiqu neifoThi vahPieBo teeBahgh
deeMeedi dithailu shiinoos phuFieth oTaepaey Oowohkoh vaiWoree ewocahPh
vapahQuo eiBirohX Goofieph Auhuaghe ooYiephi aichuJie Tieweedi aewoCaph
Ohhochai Tohzaish Aixaighi xiuGhoib teiNegho dahRohai ahhieNgi Quiuroya
AhPhorai Oovoveje ahQuiapo CooWiepo AhjoosoZ Hekuquah Ahcheavu inohCieF
quohyohW ZakohThi uoChiePa xiinieDe eebaiShe eesaaNeu osefaBaa pueYutha
ohgeiMoh Zamieshu ahmooTua aYohkiri aesaiNie thayohCh joquaiQu haeHahfa
ieRahree Ooyohpah OtaenahF OhFochua LiilooYu Eviraazu icaeQuoh luTeigoh
giethaSh Rasohchi ooChauhu xeiPiuri ojahvooM roSauCae AizaiCie doosooHu
ceigeboX bohraiBa ioJoenga Juunohne oaNgezae uongaeTh OQuahpab ahdeWape
NeopaeKa irohReik NieNeice geiKainu Ahvouquo NieZeepa Vathieyi ahveeXoh
iepheifi EpooohohY aichieFa quephatT Ezoochie Reicielu febiKies jowooZie
AeBainge oaXooDah Wachung rainiupo quiceivi Leixieki teeZahle siughoze
ulievieP eiPhiega tohoshoh eerimaoM feQuicha ievumoey quookoeX ooYaevae
Ahyohsee quaiShix Aeaeabai icaGhie Ubaishuk eeghengo Cohphooy sheSheRu
gooRooko Waperagh ooNgioBo LoosiDoh ObooxaiX eeVeecoo UiNgeiki ZooDooDu
unguoXoi eiChacho Ayeuleiz meecaeCi fohsaeDu koaPhahf Chuapaag tomuiKav
OChohXee eoNesohd AoKeiNga thulieNo KioNgahj paphaeNo IWooweib Ohxongae
laibaiRi oBohquan Oteerohn OnguReez Aogheeph Uaturoig Woeghaej voongohT
charly@salami:~$
```

Figure 2: PWGen generates whole lists of passwords, some of which are easy enough for users to memorize.

numbers, you can generate passwords that people can pronounce with some imagination. Figure 2 shows a whole list of these passwords, which are a useful compromise between convenience and security – as long as you are protecting non-privileged user accounts and not the crown jewels.

In theory, you could make this even simpler by telling PWGen not to use upper-case letters, but I wouldn't recommend it. I don't want to make it too easy for my users – after all, mind jogging is good for you. ■

SYSADMIN

De-perimeterization60

We'll look at a new approach to security.

Partition Backup64

Partition backup over the network.

```
charly@wrap:~$ Shell - Konsole <3>
2007-08-02 10:52:15,937 fail2ban.actions: WARNING [vsftpd] Ban 10.0.0.254
==> /var/log/auth.log <==
Aug 2 10:52:15 vdr vsftpd: (pam_unix) authentication failure; logname= uid=0 eu
id=0 tty=ftp ruser=charly rhost=10.0.0.254 user=charly

==> /var/log/fail2ban.log <==
2007-08-02 10:57:15,941 fail2ban.actions: WARNING [vsftpd] Unban 10.0.0.254
```

Figure 1: The IPtables blockade against the host at 10.0.0.254 started at 10:52am and ended at 10:57am.

INFO

[1] "Fail2ban" by Charly Kühnast *Linux Pro Magazine*, November 2007, pg. 63: <http://www.linuxpromagazine.com/issues/2007/84>

[2] PWGen: <http://sourceforge.net/projects/pwgen/>

THE AUTHOR

Charly Kühnast is a Unix System Manager at the data center in Moers, near Germany's famous River Rhine. His tasks include ensuring firewall security and availability and taking care of the DMZ (demilitarized zone).

