Mise en place des mots de passe sécurisés

Jean-Philippe DURAND

22 juin 2005

Installation du système de mots de passe masqués

- On installe le paquet `shadow_utils`,
- On masque la table des mots de passe `/etc/password` par la commande `pwconv`.

Contrôle sur la validité des mots de passe

- Dans `/etc/login.defs` :

```
PASS_MAX_DAYS   60
PASS_MIN_DAYS   0
PASS_MIN_LEN    8
PASS_WARN_AGE   7
```

- On fixe dans ce fichier la politique gestions des mots de passe par défaut.
- On positionne les droits 600 à ce fichier.
- On positionne les droits 644 au fichier `/etc/password`.
- On positionne les droits 644 au fichier `/etc/group`.
- On positionne les droits 400 au fichier `/etc/shadow`.

root doit être propriétaire de ces trois fichiers.

Application de ces règles aux mots de passe anciennement créés

Pour chaque utilisateur sur chacune des machines, on applique ces contraintes via la commande passwd.

```
#/bin/tcsh
set liste = "athos k2 linux nepal penjab thabor ventoux"
set liste2 = "breunoy despelin benillo leguissan casseron genzeaud bonillet"
```

```
foreach m ($liste)
 foreach g ($liste2)
  passwd -k -x 60 -w 7 -i 1 $g
 end
end
```

Configurer «pam» pour forcer le test des nouveaux mots de passe

Éditer le fichier `/etc/pam.d/system-auth` et ajouter la ligne suivante :
`password sufficient /lib/security/$ISA/pam_unix.so nullok use_authtok md5 shadow`
`use_authok` permet d'utiliser `pam_cracklib.so` pour tester les mots de passe.
`shadow` précise que les mots de passe sont masqués.
On peut, dans ce fichier, fixer un degré de complexité très poussé sur la construction du mot de passe. On choisit de se restreindre à huit caractères sans imposer de majuscules, chiffres ou caractères spéciaux.

État d'un mot de passe

La commande chage donne des informations sur l'état d'un mot de passe.

```
$ chage -l user
Minimum :       0
Maximum :       60
Avertissement : 7
Desactive :     1
Dernier changement :            jun 22, 2005
Expiration du mot de passe :    aou 21, 2005
Password Inactive:      aou 22, 2005
Account Expires:        Jamais
```

Génération de mots de passe

La commande `mkpasswd` propose des mots de passes aléatoires avec un degré de complexité adapté au besoin.

Mots de passe SAMBA

– Éditer le fichier `/etc/samba/smb.conf` .

– Modifier, si besoin, la ligne suivante :

```
Unix password sync = no
```

Mise en place d'un serveur de mots de passe

Sans utiliser `NIS`, on veut distribuer les fichiers de mots de passe de façon simple, robuste, efficace et sécurisée sur tout le réseau linux. On utilise pour cela `rsync` et `ssh` via `cron` .

Configuration de ssh

On s'assure que ssh et rsync sont bien disponibles sur toutes les machines. Les opérations suivantes doivent être effectuées sur toutes les machines du réseau.

1. Génération des clés `ssh` par la commande `ssh-keygen -t dsa` en tant que root
2. Accepter le répertoire `/root/.ssh/id_dsa`
3. Entrer une phrase-passe vide
4. Créer le fichier `/root/.ssh/config` avec le contenu suivant :

```
Host remotehost
User root
Compression yes
Protocol 2
RSAAuthentication yes
StrictHostKeyChecking no
ForwardAgent yes
ForwardX11 yes
IdentityFile /root/.ssh/id_dsa
```

5. Échanger les clefs publiques obtenues avec les autres machines. On récupère le contenu des fichiers `/root/.ssh/id_dsa.pub` de chacune des machines et on le reporte dans un fichier unique.
6. Ce fichier est ensuite copié sur chaque machine en tant que `/root/.ssh/authorized_keys2`.

ssh est maintenant prêt à fonctionner en mode non interactif (sans requérir de mots de passe) pour le compte root.

cron

Dans la crontab du serveur (`crontab -e`) on rajoute:

```
0,10,20,30,40,50 * * * * /usr/bin/rsync -e /usr/bin/ssh -a /etc/passwd /etc/shadow \
/etc/group k2:/etc/
```

autant de fois que nécessaire.
Chaque utilisateur devra saisir son mot de passe sur le serveur. Ce mot de passe sera reporté sur les autres machines automatiquement au bout de 10 minutes maximum.