Cours GNU/linux

gestions des utilisateurs

alan.simon@free.fr

Présentation

- Objectif : La séparation des privilèges :
  - Un compte sera défini par service / application / module applicatif
    - exemple : le compte apache
  - Un compte par rôle dans l'applicatif
    - Exemple : web-delivery
- Objectif : Traçabilité des actions
  - Un compte sera utilisé pour chaque intervenant (exceptions)
- Principe : la gestion des environnements
  - Un/Des Comptes et groupes
  - Un/Des Filesystème

Gestion des comptes / groupes

Commandes à connaitre :

- useradd / adduser / usermod
- passwd [user]
- groupadd
- newgrp, sg

Fichiers à connaitre :

- /etc/passwd
- /etc/group
- /etc/shells
- /etc/nsswitch.conf
- /etc/shadow / /etc/gshadow

Fichier /etc/passwd

Le compte

Le password

L'UID

Le groupe primaire : GID

Le champs gecos

Le home

Le programme de cnxn

- `# cat /etc/passwd`
- `root:x:0:0:root:/root:/bin/bash`
- `bin:x:1:1:bin:/bin:/sbin/nologin`
- `daemon:x:2:2:daemon:/sbin:/sbin/nologin`
- `adm:x:3:4:adm:/var/adm:/sbin/nologin`
- `lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin`
- `sync:x:5:0:sync:/sbin:/bin/sync`
- `shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown`
- `halt:x:7:0:halt:/sbin:/sbin/halt`
- `mail:x:8:12:mail:/var/spool/mail:/sbin/nologin`
- `uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin`
- `operator:x:11:0:operator:/root:/sbin/nologin`
- `nobody:x:99:99:Nobody:/:/sbin/nologin`
- `sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin`

Création d'un clone de root

Créer un compte toto avec la commande useradd

- lisez le man
- valider les options
- Connectez vous avec le compte

Depuis une autre session, editez le fichier /etc/passwd et changer l'uid du compte à 0

Fichier /etc/group

Structure :

- group_name
- passwd
  - Mot de passe permettant de prendre les droits du group (dans le fichier gshadow)
  - Cmd : newgrp
- GID : identifiant unique du groupe
- user_list : liste de comptes

Les groupes secondaire sont définis au login

Il font partie de l'environnement

La commande “sg” permet de changer le groupe primaire

```
root:x:0:
bin:x:1:bin,daemon
daemon:x:2:bin,daemon
sys:x:3:bin,adm
adm:x:4:adm,daemon
tty:x:5:
disk:x:6:
lp:x:7:daemon
mem:x:8:
kmem:x:9:
wheel:x:10:
mail:x:12:mail
uucp:x:14:
man:x:15:
```

Fichiers /etc/shadow & gshadow

/etc/shadow

```
root:
$6$eBwx22qHSI0D1cmy$KilNx2ZltzJEJj5REyQE
zIQPMYHvBWmYqNxPp3dpJEnylanbEAF
hHFJ3YsgJmgMmQxVq/miMdQ/wwzo1OE0yC.:1560
6:0:99999:7:::
bin:*:15513:0:99999:7:::
daemon:*:15513:0:99999:7:::
adm:*:15513:0:99999:7:::
lp:*:15513:0:99999:7:::
sync:*:15513:0:99999:7:::
```

- Login
- Encrypted Password
- Date last change
- Min age
- Max age
- Warning delay
- Locking delay
- Expiration date

/etc/gshadow

```
root:::
bin:::bin,daemon
daemon:::bin,daemon
sys:::bin,adm
adm:::adm,daemon
tty:::
disk:::
lp:::daemon
apache:!::
```

- group name
- encrypted password
- Administrators (pw members)
- members

Environnement utilisateur

Le login

Le mot de passe est vérifié

Le shell est vérifié

- Fichier /etc/shells contient les shell de login valide

Les variables sont initiées

- Source les fichier profiles

  Globale localement : /etc/profile /etc/.login

  Du compte utilisateur : ~/.profile ~/.bash_profile ~/.login

Initialisation des Variables

Shell	Système (lu en premier)	Utilisateur	Modèle /etc/skel
Bourne	/etc/profile	$HOME/.profile	local.profile
Korn	/etc/profile	$HOME/.profile puis $HOME/.kshrc	local.profile
C	/etc/.login	$HOME/.cshrc puis $HOME/.login	local.cshrc local.login
BASH	/etc/profile	$HOME/.bash_profile $HOME/.bash_login $HOME/.profile $HOME/.bashrc	
TC	/etc/rsh.cshrc /etc/csh.login	$HOME/.tcshrc ou $HOME/.cshrc $HOME/.login	
Z	/etc/zshenv /etc/zprofile /etc/zshrc /etc/zlogin	$HOME/.zshenv $HOME/.zprofile $HOME/.zlogin $HOME/.zshrc	

Gestion des environnements

Les skeldir sont des répertoirs définissants le contenu initial du home utilisateur copié lors de la création d'un compte :

```
$ ls -al /etc/skel/
total 32
drwxr-xr-x   2 root root  4096 2011-02-14 16:21 .
drwxr-xr-x 130 root root 12288 2013-03-11 07:26 ..
-rw-r--r--   1 root root   220 2010-04-19 03:51 .bash_logout
-rw-r--r--   1 root root  3103 2010-04-19 03:51 .bashrc
-rw-r--r--   1 root root   675 2010-04-19 03:51 .profile
-rw-r--r--   1 root root  1791 2010-05-04 19:20 .Xdefaults
```

Gestion des environnments utilisateurs :

- télédistribution des home dir
- automount NIS (obsolète)

Gestion des environnements applicatifs :

- Gestion des variables d'environnements spécifique (exemple : ORACLE_HOME)

Processus d'Authentification

PAM : Plugable Authentification Module

Authentification unifiée

Librairie pour les developpements

Politique d'authent parametrable

4 groupes de gestion d'authent

- account : taches validant du compte
- auth (entification) : taches vérifiant l'identité
- password : taches validant des update de l'auth
- session : taches générique d'accès à un service executé avant et/ou après l'accès

Modulaire

- Plusieurs operations peuvent être effectuées pour valider l'accès
- Dans un ordre précis car chacune pouvant être un condition nécessaire ou suffisante
  - Necessaire : Required : juste à valider
  - Requis : Requisits : option indispenssable (permet de notifier la raison du refus)
  - Suffisant : ne necessite pas d'autre validation (on sort de la chaine de validation avec succes)
  - Optionnel : le résultat est ignoré (sauf si le seul de la chaine)

PAM : Exemple

auth required pam_securetty.so

Ce module valide la règle securetty a l'authent : si le fichier /etc/securetty existe root ne peu se connecter que depuis les tty définis dans ce fichier)

auth required pam_unix.so nullok

Ce module demande le mot de passe et le valide l'option nullok indique que si la référence est un mot de passe vide alors la connexion est authorisé

auth required pam_nologin.so

Ce module valide la règle nologin, si le fichier /etc/nologin existe seul root peut se connecter

account required pam_unix.so

Ce module valide l'ensemble des règles standard unix de vérififcation des comptes

password required pam_cracklib.so retry=3

Impose un changement de mot de passe si le compte est expiré et valide qu'il ne soit pas un mot de passe trivial (propose 3 reessais)

password required pam_unix.so shadow nullok use_authtok

Utilisation du module std unix pour le changement de mot de passe, user_authok : permet de ne pas redemander le mot de passe d'orrigine s'il à déja été validé au préalable (ligne 2)

session required pam_unix.so

Gestion standard unix de la session : comme le log la connexion et la deconnexion

Force password complexity

/etc/pam.d/system-auth

password requisite pam_cracklib.so try_first_pass

password requisite pam_cracklib.so try_first_pass retry=3 minlen=14 ucredit=-1 dcredit=-1 ocredit=-1 lcredit=-1

- Lock the account:
  - usermod -L johndoe
- Expire their current password:
  - chage -d 0 johndoe
- Unlock the account:
  - usermod -U johndoe
- Validate:
  - chage -l johndoe

- retry=N : Prompt user at most N times before returning with error. The default is 1.
- minlen=N : The minimum acceptable size for the new password (plus one if credits are not disabled which is the default). In addition to the number of characters in the new password, credit (of +1 in length)
- reject_username : Check whether the name of the user in straight or reversed form is contained in the new password. If it is found the new password is rejected.
- dcredit=N : (N >= 0) This is the maximum credit for having digits in the new password.
- lcredit=N : (N >= 0) This is the maximum credit for having lower case letters in the new password.
- ocredit=N : (N >= 0) This is the maximum credit for having other characters in the new password.
- ucredit=N : (N >= 0) This is the maximum credit for having upper case letters in the new password.

  If you have less than or N digits, each digit will count +1 towards meeting the current minlen value.

TP

Script de création de compte Utilisateur ou Applicatif

- Mise en place d'un répertoire /root/exploit
- Création de 2 scripts SIMPLE qui standardise la création des compte
  - Utilisateur : home dir standard, gestion de la complexité du mot de passe forcer le changement de mot de passe
  - Applicatif : imposer la définition d'un home, invitation dans un groupe app