TP4 : cron, pam et quotas

Vous devez rédiger un compte-rendu de ce TP et le rendre à la fin de la séance.

Préliminaires

Avant toute chose, il vous faut réinstaller une slackware sur votre machine, puis désinstaller les paquets `apache` et `openldap`.

1 Automatisation de commandes avec `cron` et `at`

La commande `at` permet de programmer l'exécution d'une tâche donnée à un instant donné. La commande `crontab` permet quant à elle de programmer l'exécution d'une tâche à intervales réguliers. La différence entre les deux est que les commandes lancées par `at` ne s'exécutent qu'une seule fois. Référez-vous aux pages de manuel pour plus de détail.

► **Question 1.** Programmez l'exécution de la commande "echo bonjour|wall" pour dans une minute, et observez le résultat.

► **Question 2.** Programmez l'exécution de la commande "halt" pour dans 5 minutes, puis trouvez une solution pour éviter que votre machine ne s'arrête.

► **Question 3.** Programmez pour à la fin de la séance l'arrêt de votre machine en utilisant la commande `shutdown +5` et non `halt`. Quelle est la différence ? A quoi cela peut-il servir (cf l'option `-c` de shutdown)

► **Question 4.** Utilisez la commande wall pour programmer l'affichage de l'heure sur tous les terminaux toutes les demi-heure.

★ **Checkpoint 1.** Faites vérifier par l'encadrant que le carillon de la dernière question fonctionne.

2 Gestion des utilisateurs

2.1 Utilisation de login.defs

Les outils « shadow password » sont configurés par l'intermédiaire du fichier `/etc/login.defs`. Pour plus d'informations, référez vous à la page de manuel login.defs(5).

Apportez les modifications nécessaires à votre configuration pour :

► **Question 5.** Faire en sorte que les UID des nouveaux utilisateurs soient compris entre 2048 et 4096.

► **Question 6.** Forcer les utilisateurs à changer de mot de passe tous les mois, en les prévenant 10 jours avant la date fatidique, mais sans invalider le compte des utilisateurs ne s'étant pas pliés à cette règle.

► **Question 7.** Autoriser les utilisateurs à changer leur shell par défaut sans avoir à taper leur mot de passe.

► **Question 8.** Forcer les utilisateurs à utiliser des mots de passe de 6 caractères ou plus.

► **Question 9.** Afficher des étoiles à la place des caractères tapés lorsqu'un utilisateur se connecte.

Créez un nouvel utilisateur et testez les changements apportés.

★ **Checkpoint 2.** Faites vérifier par l'encadant le bon fonctionnement de la dernière question.

2.2 Compilation des Plugable Authentication Modules (PAM)

Il s'agit d'un mécanisme permettant de modifier l'authentification sur le système sans avoir à modifier les applications en dépendant. Il est ainsi possible de demander aux utilisateurs d'utiliser une carte à puce pour pouvoir se logger au système sans avoir à modifier l'application `login`.

Ce système est inclus par défaut dans la plupart des distributions de linux, sauf Slackware car son auteur principal (Patrick J. Volkerding) considère que les avantages apportés ne sont pas suffisant pour justifier les riques introduits, par exemple en cas de mauvaise configuration.

Nous allons mettre en place un système utilisant une base de données LDAP pour stocker les mots de passe. LDAP étant intérogeable à distance, cette approche est très souvent utilisée pour n'avoir qu'une seule base des utilisateurs pour tout un réseau de machines (comme à l'ESIAL). Nous utiliserons la même base pour les authentifications du serveur web controlant l'accès à des pages protégées.

⇒ Ouvrez plusieurs consoles, et ne les fermez pas avant le checkpoint suivant⇐
Les manipulations suivantes peuvent vous empêcher de vous connecter si vous faites une fausse manoeuvre. Les consoles supplémentaires peuvent donc s'avèrer précieuse pour corriger vos erreurs.

2.2.1 Compilation de libpam (`ftp://ftp.kernel.org/pub/linux/libs/pam/pre/library/`)

(le \ de fin de ligne signifie que la ligne de commande continue sur la ligne suivante)

```
./configure --enable-static-libpam --with-mailspool=/var/mail \
  --enable-read-both-confs --sysconfdir=/etc &&
make && make install &&
mv -v /lib/libpam.a /lib/libpam_misc.a /lib/libpamc.a /usr/lib &&
ln -v -sf ../../lib/libpam.so.0.79 /usr/lib/libpam.so &&
ln -v -sf ../../lib/libpam_misc.so.0.79 /usr/lib/libpam_misc.so &&
ln -v -sf ../../lib/libpamc.so.0.79 /usr/lib/libpamc.so
```

▶ **Question 10.** A votre avis, pourquoi installer cette bibliothèque dans `/lib` et non dans `/usr/lib` ?

Contenu de /etc/pam.d/other

```
1 auth            required        pam_unix.so     nullok
2 account         required        pam_unix.so
3 session         required        pam_unix.so
4 password        required        pam_unix.so     nullok
```

▶ **Question 11.** En vous aidant de pam(8), expliquez le sens de chaque ligne de `/etc/pam.d/other`

2.3 shadow (`ftp://ftp.pld.org.pl/software/shadow/`) et PAM

L'objectif est d'utiliser les PAM dans les programmes `login`, `su`, `passwd` et tous les autres de shadow.

```
./configure --libdir=/lib --enable-shared --with-libpam --without-libcrack
make && make install &&
mv -v /usr/bin/passwd /bin &&
mv -v /lib/libshadow.*a /usr/lib &&
rm -v /lib/libshadow.so &&
ln -v -sf ../../lib/libshadow.so.0 /usr/lib/libshadow.so
```

Contenu de /etc/pam.d/login

```
1  auth        requisite      pam_securetty.so
2  auth        requisite      pam_nologin.so
3  auth        required       pam_env.so
4  auth        required       pam_unix.so
5  account     required       pam_access.so
6  account     required       pam_unix.so
7  session     required       pam_motd.so
8  session     required       pam_limits.so
9  session     optional       pam_mail.so      dir=/var/mail standard
10 session     optional       pam_lastlog.so
11 session     required       pam_unix.so
12 password    required       pam_unix.so      md5 shadow
```

▶ **Question 12.** Expliquez 6 lignes de votre choix dans de ce fichier `/etc/pam.d/login`

Contenu de /etc/pam.d/passwd

```
password    required       pam_unix.so      md5 shadow
```

Contenu de /etc/pam.d/su

```
auth        sufficient      pam_rootok.so
auth        required        pam_unix.so
account     required        pam_unix.so
session     optional        pam_mail.so     dir=/var/mail standard
session     required        pam_unix.so
```

Contenu de /etc/pam.d/chage

```
auth        sufficient      pam_rootok.so
auth        required        pam_unix.so
account     required        pam_unix.so
session     required        pam_unix.so
password    required        pam_permit.so
```

Les fichiers pour `chpasswd newusers groupadd groupdel groupmod useradd userdel usermod` sont identiques à `/etc/pam.d/chage`.

★ **Checkpoint 3.** Faites vérifier par l'encadrant que vous pouvez à nouveau vous logger.

2.4 Installer OpenLDAP

2.4.1 Compilation

```
CPPFLAGS=-I/usr/include/db4 ./configure  --prefix=/usr/local/ldap \
  --with-readline --with-threads \
  --enable-syslog --enable-aci --enable-cleartext --enable-crypt \
  --libexecdir=/usr/local/ldap/sbin --sysconfdir=/usr/local/ldap
make depend && make && make install
```

(l'écriture `VARIABLE=valeur commande` permet de modifier une variable d'environnement pour cette commande seulement et non de manière définitive)

Ajoutez `/usr/local/ldap/lib` à `/etc/ld.so.conf` puis faites le nécessaire.

2.4.2 Configurer OpenLDAP

Contenu de /usr/local/ldap/etc/openldap/slapd.conf

```
1  include /usr/local/ldap/etc/openldap/schema/core.schema
2  include /usr/local/ldap/etc/openldap/schema/cosine.schema
3  include /usr/local/ldap/etc/openldap/schema/inetorgperson.schema
4  include /usr/local/ldap/etc/openldap/schema/nis.schema
5  include /usr/local/ldap/etc/openldap/schema/openldap.schema
6  schemacheck on # Force la vérification de la structure des ajouts
7  loglevel 256 # Voir slapd.conf(5) pour les valeurs possibles
8  ...
9  database=bdb
10 suffix="dc=esial.uhp-nancy,dc=fr"
11 rootdn="cn=Admin,dc=esial.uhp-nancy,dc=fr"
12 rootpw ILoveMummy
13 ...
14 access to attr=userPassword
15   by self write
16   by anonymous read # Voir la partie "La suite de l'histoire"
17   by dn="cn=Admin,dc=esial.uhp-nancy,dc=fr"
18   by * none
19 access to *
20   by * read
21   by dn="cn=Admin,dc=esial.uhp-nancy,dc=fr"
```

► **Question 13.** A votre avis, que veulent dire les lignes 15-22 ? (question subsidiaire pour le sens des autres lignes)

2.4.3 Initialiser la base LDAP

Contenu de base.ldif

```
dn: dc=esial.uhp-nancy,dc=fr
objectClass: top
objectClass: organization
objectClass: dcObject
dc: esial.uhp-nancy
o: Ecole Superieure Informatique et Applications de Lorraine

dn: ou=People,dc=esial.uhp-nancy,dc=fr
ou: People
objectClass: organizationalUnit

dn: ou=Group,dc=esial.uhp-nancy,dc=fr
ou: Group
objectClass: organizationalUnit
```

Utilisez ce fichier pour peupler la base (l'option `-c` permet de remplacer l'existant) puis vérifiez que cela a fonctionné :

```
/usr/local/ldap/sbin/slapadd -l base.ldif -f /usr/local/ldap/etc/openldap/slapd.conf
/usr/local/ldap/sbin/slapcat -f /usr/local/ldap/etc/openldap/slapd.conf
```

2.4.4 Démarrage manuel et automatique

Démarrez le démon manuellement :

```
/usr/local/ldap/sbin/slapd -f /usr/local/ldap/etc/openldap/slapd.conf
```

▶ **Question 14.** Comment vérifier que le serveur fonctionne (qu'un processus slapd existe) ?

▶ **Question 15.** Comment tuer le serveur avant de le relancer ?

▶ **Question 16.** Sur le modèle de `/etc/rc.d/rc.gpm`, faites un `/etc/rc.d/rc.ldap` puis modifiez `rc.M` pour l'utiliser.

2.4.5 Ajouter un utilisateur à la base LDAP

1. Ajoutez un utilisateur avec `useradd` et changez son mot de passe avec `passwd`.
2. Téléchargez les outils de migration depuis `http://www.padl.com/OSS/MigrationTools.html`
3. Modifiez `migrate_common.ph` pour configurer les scripts :

   Modification à migrate_common.ph

   ```
   $DEFAULT_MAIL_DOMAIN = "esial.uhp-nancy.fr";
   $DEFAULT_BASE = "dc=esial.uhp-nancy,dc=fr";
   ```

4. Convertissez le contenu actuel de vos fichiers.

   ```
   ./migrate_passwd.pl /etc/passwd > passwd.ldif
   ./migrate_group.pl /etc/group > group.ldif
   ```

5. Éditez `passwd.ldif` pour ne garder que l'utilisateur que vous venez de créer.
6. Ajoutez ces fichiers à la base LDAP en tant qu'administrateur :

   ```
   /usr/local/ldap/bin/ldapadd -f /tmp/user.ldif -x \
     -D "cn=Admin,dc=esial.uhp-nancy,dc=fr"  -w ILoveMummy
   ```

2.5 Authentification Apache sur LDAP

2.5.1 (re)Compilation d'Apache

```
./configure --prefix=/usr/local/apache --enable-module=most --enable-shared=max \
  --with-ldap=yes --with-ldap-include=/usr/local/ldap/include \
  --with-ldap-lib=/usr/local/ldap/lib --enable-ldap=static --enable-auth-ldap=static
make && make install
```

2.5.2 Configuration d'Apache

Dans la section <Directory "/usr/local/apache/htdocs"> du fichier /usr/local/apache/conf/httpd.conf, changez `AllowOverride None` en `AllowOverride AuthConfig` et relancez le serveur.

Contenu de /usr/local/apache/htdocs/.htaccess

```
AuthName "Tests sur l'authentification avec LDAP"
AuthType Basic
AuthLDAPUrl "ldap://localhost:389/ou=People,dc=esial.uhp-nancy,dc=fr?uid?sub"
require valid-user
```

★ **Checkpoint 4.** Faites vérifier par l'encadrant que seul l'utilisateur créé a accès à la page.

2.6 Authentification PAM sur LDAP

► **Question 17.** Faites en sorte que l'utilisateur ne soit recensé que dans la base LDAP. De quel(s) fichier(s) faut-il le retirer ? Quelles sont les modifications à apporter ?

2.6.1 nss_ldap (ftp://ftp.padl.com/pub/nss_ldap.tgz)

NSS (*Name Service Switch*, commutateur de services de nommages) permet de fournir à UNIX divers services de correspondances entre noms : UID *vs.* nom d'utilisateur, IP *vs.* nom d'hôte, *etc.*

```
./configure --with-ldap-dir=/usr/local/ldap && make
cp nss_ldap.so /lib/libnss_ldap.so
ln -s /lib/libnss_ldap.so /lib/libnss_ldap.so.2
```

Modification de /etc/nsswitch.conf

```
passwd:     files ldap
shadow:     files ldap
group:      files ldap
```

2.6.2 pam_ldap (ftp://ftp.padl.com/pub/pam_ldap.tgz)

```
./configure --with-ldap-dir=/usr/local/ldap && make && cp pam_ldap.so /lib/security/
```

Contenu de /etc/ldap.conf

```
host 127.0.0.1
base dc=esial.uhp-nancy,dc=fr
ldap_version 3
```

Ajout à /etc/pam.d/login

```
auth       sufficient   pam_ldap.so use_first_pass
account    sufficient   pam_ldap.so
password   sufficient   pam_ldap.so
```

► **Question 18.** Modifiez ce qui doit l'être pour permettre à root de prendre l'identité de l'utilisateur avec `su`.

★ **Checkpoint 5.** Faites vérifier par l'encadrant que l'utilisateur créé peut se logger.

2.6.3 La suite de l'histoire

Nous avons mis en place un système de gestion des utilisateurs UNIX par une base LDAP fonctionnelle. Cependant, la sécurité offerte par notre solution n'est absolument pas suffisante, et plusieurs points seraient à renforcer pour un déploiement sur réseau réel :

- Le protocole LDAP lui-même n'est pas sécurisé et la plupart des informations circulent en clair sur le réseau. Il conviendrait donc d'utiliser SSL ou TLS pour crypter les communications LDAP.
- Le mot de passe de l'administrateur LDAP est en clair dans le fichier : slapd.conf(5) et slappasswd(8)
- Le serveur LDAP devient un élément crucial de l'architecture, et plus rien ne fonctionne sans lui. Il convient donc de mettre en place des serveurs de secours (avec slurp(8)).
- À la ligne 16 du fichier `slapd.conf`, nous avons écrit que les mots de passe cryptés sont lisibles par tous. Il serait préférable de mimer le comportement de shadow avec `by anonymous auth`

3 Quotas sur système de fichiers

Les quotas permettent de restreindre l'utilisation du disque par les utilisateurs. Il est possible de limiter l'espace dique utilisé par chaque utilisateur (ou groupe), mais également le nombre d'*inœuds* utilisé par chacun. Si le système compte plusieurs systèmes de fichiers (plusieurs partitions), chacun d'entre eux a des quotas spécifiques.

Le système de gestion des quotas se découpe en un module noyau et des outils en espace utilisateur.

3.1 Installation

▶ **Question 19.** Vérifiez (dans `/boot/config-votre-noyau`) que l'option concernant les quotas est activée dans votre noyau. Comment faites-vous ?

▶ **Question 20.** Installez le paquet `quota` depuis le CD.

Vous pouvez maintenant consulter la documentation : `/usr/share/doc/quota-3.12/quotadoc.html`

▶ **Question 21.** Quelle est la différence entre « softlimit » et « hardlimit » ? Qu'est-ce que le délai de grâce ?

3.2 Configuration et mise en place

Ajoutez l'option `usrquota` à vos partitions dans `/etc/fstab` :

```
/dev/hda1  /  ext3  defaults,usrquota  1  1
```

Créez un fichier `aquota.user` à la racine de chacun de vos systèmes de fichiers (`/aquota.user` ; `/home/aquota.user` ; . . .). Changez les droits de ces fichiers en 600.

▶ **Question 22.** Quel est le script de démarrage chargé d'activer les quotas ? Observez le code correspondant. Sous quelle condition active-t-il ce mécanisme ? Vérifiez que vous la remplissez puis redémarrez.

3.3 Utilisation

▶ **Question 23.** Avec `edquota`, placez respectivement les limites douce et dure de votre utilisateur à 50 Mo et 60 Mo (les blocs font 1 ko).

★ **Checkpoint 6.** Faites vérifier à l'encadrant le bon fonctionnement de ces limites.

Félicitations, vous avez fini.