Table des matières

Questions :

1) PAM n'est pas un daemon. Tous les programmes qui sont des daemon ont un PPID = 1

```
test@214-10 : ~
$ ps -fe | grep pam
test      1621  1620  0 13:01 ?        00:00:00 (sd-pam)
test      5231  5202  0 13:15 pts/0    00:00:00 grep pam
```

En violet on peut voir que le PPID de pam est égale à 1620 et 5202 donc ce n'est pas un daemon.

2) Pour afficher les droits complets de tous les programmes utilisant pam dans /bin il faut d'abord savoir quels programmes sont en communs entre /etc/pam.d et /bin. Pour cela on peut faire la commande suivante :

```
root@214-10 : /home/test
# ldd /bin/* | grep -B 5 libpam.so | grep -E "(libpam|:)"
/bin/login:
     libpam.so.0 => /lib/x86_64-linux-gnu/libpam.so.0
(0x00007f24cfcf5000)
/bin/su:
     libpam.so.0 => /lib/x86_64-linux-gnu/libpam.so.0
(0x00007f821e2ae000)
     libpam.so.0 => /lib/x86_64-linux-gnu/libpam.so.0
(0x00007f9b29d0f000)
```

Une fois qu'on récupéré on a plus qu'à afficher les droits des programmes :

```
root@214-10 : /home/test
# ls -l /bin/login /bin/su
-rwxr-xr-x 1 root root 56760 juil. 27  2018 /bin/login
-rwsr-xr-x 1 root root 63568 janv. 10  2019 /bin/su
```

On voit que l'utilisateur root a tous les droits, les users peuvent lire et exécuter les fichiers et que les autres ne peuvent qu'exécuter

3) La commande apropos permet de donner la description des pages du man. Ici il donne la liste de tous les fichiers qui interagissent avec PAM. On grep ensuite «PAM module» pour n'avoir que la liste des modules

```
root@214-10 : /home/test
# apropos pam |grep "PAM module"
pam_access (8)       - PAM module for logdaemon style login access
control
pam_cap (8)          - PAM module to set inheritable capabilities
pam_debug (8)        - PAM module to debug the PAM stack
pam_deny (8)         - The locking-out PAM module
pam_echo (8)         - PAM module for printing text messages
pam_env (7)          - PAM module to set/unset environment
variables
pam_exec (8)         - PAM module which calls an external command
pam_ftp (8)          - PAM module for anonymous access module
pam_group (8)        - PAM module for group access
pam_issue (8)        - PAM module to add issue file to user prompt
pam_lastlog (8)      - PAM module to display date of last login
and perform i...
pam_limits (8)       - PAM module to limit resources
pam_mkhomedir (8)    - PAM module to create users home directory
pam_namespace (8)    - PAM module for configuring namespace for a
session
pam_pwhistory (8)    - PAM module to remember last passwords
pam_rhosts (8)       - The rhosts PAM module
pam_selinux (7)      - PAM module to set the default security
context
pam_sepermit (8)     - PAM module to allow/deny login depending on
SELinux en...
pam_shells (8)       - PAM module to check for valid login shell
pam_time (8)         - PAM module for time control access
pam_umask (8)        - PAM module to set the file mode creation
mask
pam_userdb (8)       - PAM module to authenticate against a db
database
pam_warn (8)         - PAM module which logs all PAM items if
called
pam_xauth (8)        - PAM module to forward xauth keys between
users
```

4) Je cat un fichier dans /etc/pam.d :

```
root@214-10 : /home/test
# cat /etc/pam.d/atd
#
# The PAM configuration file for the at daemon
#

@include common-auth
@include common-account
session    required   pam_loginuid.so
@include common-session-noninteractive
session    required   pam_limits.so
auth required  pam_env.so user_readenv=1
```

La 1ère colonne est affichée en violet. Cela correspond au service du module

5) La 2ème colonne est affichée en bleue. Cela correspond au control-flag. Il y a différentes valeurs telles que « requiered ; requisite ; sufficent ; optional ; include ». Ici le control-flag est « requiered ». Tous les modules méthodes required doivent réussir pour que la vérification soit accordée. L'utilisateur est prévenu à la fin du traitement de la pile.

6) Pour modifier le message de bienvenue de ssh, il faut modifier le fichier /etc/ssh/sshd_config

On doit décommenter la ligne « banner ». Après banner, on met le nom du fichier avec le texte que l'on souhaite mettre

Ici :

```
Banner /etc/ssh/test
```

Dans le fichier test, j'ai écris «Salut»

Quand je fais un ssh, on voit alors :

```
root@214-10:/etc/ssh# ssh root@214-11
Salut
root@214-11 password:
....
```

Il affiche le message lorsqu'on tente la connexion

7) Pour n'autoriser que certains utilisateurs à utiliser ssh avec PAM, il faut modifier le fichier /etc/pam.d/sshd

Dans celui-ci, on rajoute une ligne avec le service « auth » pour authentifier la personne.

On dit que c'est un fichier de liste

On dit aussi que ce qui est dans le fichier est un username

On dit qu'on autorise cet user

Le fichier où sont les user se trouve à : /....

Cela donne :

auth requisite pam_listfile.so item=user sense=allow file=/etc/ssh/allow_ssh

On rempli le fichier /etc/ssh/allow_ssh de nom d'utilisateurs (1 par ligne)

Si l'on essaie de ssh et qu'on est pas dans le fichier, cela ne fonctionnera pas

8)