Processus de login sous Linux

A. Format du fichier "/etc/shadow"

Sur les systèmes Linux modernes, les mots de passe sont stockés dans le fichier "/etc/shadow", sous leur forme chiffrée.
Contrairement à l'ancien fichier "/etc/passwd" qui stockait les mots de passe sous Linux, le
fichier "/etc/shadow" est uniquement accessible par l'utilisateur "root" pour des raisons de sécurité (les hashs des mots de passe ne sont pas censés être accessibles par tous).
Cette nouvelle méthode est apparue en 1988 avec le développement de System V 3.2.

Le fichier "/etc/shadow" recense les comptes utilisateurs mais aussi les comptes de services (daemon).

```
backup:*:15710:0:99999:7:::
bin:*:15710:0:99999:7:::
daemon:*:15710:0:99999:7:::
Debian-exim:!:15710:0:99999:7:::
Debian-gdm:*:15710:0:99999:7:::
games:*:15710:0:99999:7:::
gnats:*:15710:0:99999:7:::
guest:$6$/fHlwNuG$A4ofEtOFtLXkACB2h9XrBFMA3oyu2Xjx9xJbeVwt6ZjMJjltGbzhy2qbf8QpnsO1U2erUPbgtJFkO1.rPLVx0/:15725:0:99999:7:::
haldaemon:*:15717:0:99999:7:::
irc:*:15710:0:99999:7:::
lambda:$5$G9juS09t$zeBhyVdKin5lVIgbgSLXsOEzF97aO2Npc86vryVjDf.:15725:0:99999:7:::
libuuid:!:15710:0:99999:7:::
list:*:15710:0:99999:7:::
lp:*:15710:0:99999:7:::
mail:*:15710:0:99999:7:::
man:*:15710:0:99999:7:::
messagebus:*:15710:0:99999:7:::
news:*:15710:0:99999:7:::
nobody:*:15710:0:99999:7:::
proxy:*:15710:0:99999:7:::
root:$6$mYSVclH7$PCiYwn4dcv0sxY9.5gPOH1MiaqYqjTgbLJNH5N2.d/svQT9WBoVzOGo6CAeJWa9mUZaMbK4BTonWvleweKIt20:15725:0:99999:7:::
snoop:$1$ptCp5rLe$y2ACxwIny032raCpJ0pO30:15725:0:99999:7:::
sshd:*:15710:0:99999:7:::
statd:*:15710:0:99999:7:::
sync:*:15710:0:99999:7:::
sys:*:15710:0:99999:7:::
usbmux:*:15710:0:99999:7:::
uucp:*:15710:0:99999:7:::
www-data:*:15710:0:99999:7:::
```

A. Format du fichier "/etc/shadow"

Chaque compte utilisateur, se décrit de la façon suivante :

login:idrounds=<N>$salt$hash:

id :	algorithme utilisé pour générer le hash du mot de passe
rounds :	paramètre optionnel, il spécifie le nombre de rondes que la fonction de hachage devra effectuer
salt :	valeur pseudo-aléatoire encodée en base64 et d'une taille maximale de 16 caractères. Son intérêt est de rajouter un aléas sur le mot de passe, afin que deux utilisateurs ayant le même mot de passe, n'aient pas le même hash dans le fichier "/etc/shadow". Cette technique permet également de rendre plus difficile les attaques sur les mots de passe par rainbow tables.
hash :	Hash du mot de passe

Id	Fonction	Taille du hash (caractères)	Nombre de rondes
1	DES	11	16
2a	MD5	22	1000
md5	Blowfish	-	16
5	Sun MD5	-	-
6	SHA-256	43	Défaut : 5000 Min : 1000 Max : 999 999 999
	SHA-512	86	Défaut : 5000 Min : 1000 Max : 999 999 999

B. Configuration du système d'exploitation

La fonction utilisée pour générer les hashs des mots de passe des utilisateurs est définie dans le fichier "/etc/pam.d/common-password".
Il est possible de modifier se fichier, pour choisir l'une des fonctions citées dans le tableau précédent.
Il faut ensuite mettre à jour ces informations avec la commande "pam-auth-update".