Architecture d'un système d'exploitation (UE S3)

TP4

Introduction à la sécurité informatique en environnement HPC

Etudiant : Romain Pereira *Encadrant :* M. F. Combeau

17/11/2018

Table des matières

1 Réponses aux questions 1 à 22 (faites en cours)

4. Pour se connecter, on a utilisé l'authentification système, à savoir, les **Pluggable Authentication Modules (PAM)**

5. Le mot de passe *root* est stocké dans le fichier '/etc/shadow' sous forme d'un hachage. Le mot de passe est haché avant d'être stocké car il est stocké localement (chaque machine connecté au réseau possède le fichier '/etc/shadow' localement).

6. Je ne peux pas déterminer facilement le mot de passe de *Bob*, car il est également stocké sous forme de hash. Cependant, à l'aide d'une méthode de brute force, on pourrait eventuellement déterminer des chaîne de caractères qui ont le même hash que celui de *Bob*. Le mot de passe de *Bob* serait donc potentiellement l'une de ces chaînes de caractères, ou pas.

On ne peut pas déterminer le mot de passe d'*Alice*, car elle n'en a pas. En effet, le champ devant correspondre à son mot de passe dans le fichier '/etc/shadow' est ***** (ou **!!**). Les fonctions de hachages utilisées par les PAM ne donneront jamais des hashs avec ces caractères ('*' et '!'). En spécifiant des caractères impossibles à obtenir par hachage, on désactive de façon indirecte l'authentification par mot de passe pour l'utilisateur : jamais un mot de passe ne donnera ce hash. L'utilisateur est en quelque sorte 'banni'.

7. Si l'on passe cette ligne de **sufficient** à **required**, alors *root* ne pourra plus se logger s'authentifier. En effet, l'identifiant utilisateur (*uid*) de *root* vaut 0. A la ligne suivante, on refuse l'authentification des utilisateurs dont l'uid est inférieur à 1000, le test ne passera donc pas. est donc inférieur à 1000 : les tests suivant ne passeront pas.

Finalement, *root* ne pourra plus se logger (à cause de la ligne *pam_ deny.so*)

8. Oui, on arrive à se connecter sur le compte de *Bob* à partir du compte *root*

Listing 1 – bash version

```
> less /var/log/secure
[...]
Accepted password for bob form ::1 port 47404 ssh2
pam_unix(sshd:session) : session opened for user bob by (uid=0)
[...]
```

La connexion sur le compte *bob* à partir de l'utilisateur *root* (uid=0) est bien tracée dans les logs.

10.

11.

12.

13.

14.

15.

16.

17.

18.

19.

20.

21.

22.

2 Réponses aux questions XX à YY (bonus)