A Introduction et définitions

Tout système d'information devrait faire l'objet d'une politique de sécurité définie par la direction et mise en place par l'administrateur du système informatique. Un document décrivant l'utilisation normale et anormale du système informatique doit être établi, de façon à prévenir toute utilisation non autorisée des matériels informatiques, et à assurer les utilisateurs légitimes contre les interruptions de service.

La sécurité doit accompagner le système dans un environnement en constante évolution ; ce n'est donc pas une tâche ponctuelle mais un travail quotidien de surveillance et de mise à niveau de la protection pour l'administrateur.

Plusieurs aspects de la sécurité existent, le niveau de sécurité global du système étant celui du point le plus faible du système :

- sécurité physique ;
- sécurité réseau ;
- authentification ;
- autorisation.

Cependant la sécurité ayant un coût, la politique définie doit être en adéquation avec l'importance des données à protéger.

> *Un certain nombre de conseils et de règles indiquées dans ce chapitre sont applicables à d'autres systèmes d'exploitation que GNU/Linux.*

1 Sécurité physique

La sécurité physique est trop souvent négligée alors que ce doit être le premier point à considérer. Aussi robuste que soit le système d'exploitation utilisé, il ne peut se prémunir de phénomènes physiques, comme le vol d'une unité de disque de la part d'une personne mal intentionnée par exemple.

Il faut donc restreindre l'accès au matériel informatique ; pour cela, plusieurs moyens s'offrent à vous :

- verrous aux portes et codes d'accès ;
- identification du personnel ;
- protection physique du câblage.

Au niveau de l'environnement, il faut penser à :

- protéger le réseau électrique des coupures et des surtensions (onduleur) ;
- installer les équipements de lutte contre le feu adaptés (extincteurs) ;
- réguler la température et l'humidité de la salle informatique (climatisation).

Enfin, si l'interruption de service est un élément pénalisant pour l'activité, il peut être utile de prévoir des pièces de rechange pour minimiser le temps d'immobilisation dû à une panne matérielle.

Rappelons ici que la sauvegarde est le meilleur moyen de prévenir la perte des données si celle-ci est effectuée rigoureusement. Il faut bien sûr veiller à stocker les médias de sauvegarde hors site.

2 Sécurité réseau

La sécurité réseau sous Linux est un élément important car ce système est généralement utilisé comme serveur (Web, messagerie électronique, serveur de fichiers...).

Les outils disponibles de surveillance et d'analyse du trafic réseau sont nombreux et variés dans le monde du logiciel libre. On nomme généralement au sein de l'équipe informatique un administrateur réseau ayant la lourde tâche de mettre en place, de maintenir et de protéger les systèmes informatiques connectés au réseau d'entreprise.

Ce livre ne traitant pas des services réseau sous Linux, cet aspect de la sécurité ne sera pas détaillé ici.

3 Hackers et crackers

À l'origine, le terme "hacker" désignait les "gourous informatiques" ayant contribué à l'émergence des systèmes Unix et les développeurs (de talent) en langage C de la première heure.

Aujourd'hui, probablement par un manque de connaissances de la part des médias, ce titre est donné à toute personne cherchant à s'introduire ou à contourner un système informatique. On peut néanmoins distinguer le "hacker" du "cracker".

Un hacker est une personne voulant satisfaire sa curiosité sans chercher à causer des dommages ou des torts à quiconque ; cependant, il peut causer des préjudices accidentellement.

Un cracker est une personne à la recherche d'un gain, qui cherche par exemple à :

- accéder aux ressources du système ;
- accéder aux données ;
- faire de la publicité non sollicitée (SPAM) ;
- prendre une revanche.

Les motivations qui peuvent amener ces personnes à s'introduire sur un système informatique sont diverses :

- curiosité ;
- challenge, prestige ;
- espionnage industriel, politique : informations confidentielles, propriété intellectuelle, propriété logicielle ;
- utilisation des ressources : espace disque, temps CPU, bande passante ;
- argent : numéros de cartes bleues, bases de données de sites marchands ;
- préparation pour l'attaque d'autres sites : DDoS (*Distributed Denial of Service*), envoi de mails non désirés (SPAM).

Quoi qu'il en soit, l'administrateur ne doit pas faire de distinction entre ces deux catégories de personnes. En effet, il est difficile de les différencier et les deux peuvent causer des dégâts.

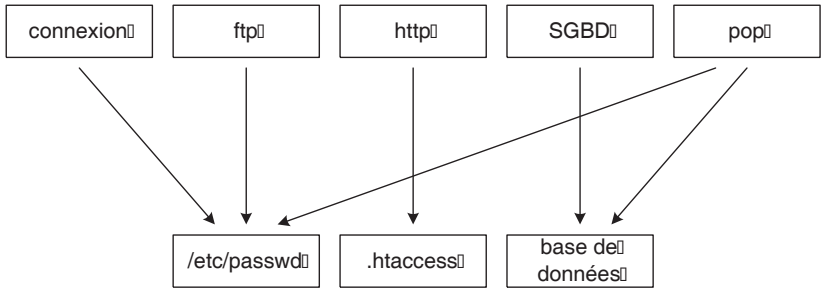
B Authentification

L'authentification permet d'établir l'identité de l'utilisateur cherchant à employer les ressources du système informatique. Il existe plusieurs systèmes d'authentification : nom d'utilisateur/mot de passe, clé de cryptage publique, carte à puce, caractères physiologiques...

1 PAM

Initialement développé par Sun Microsystems, PAM (*Pluggable Authentication Modules*) a été adapté pour Linux. Il est devenu le système actuel d'authentification.

Auparavant, chaque application utilisait sa propre méthode d'authentification :

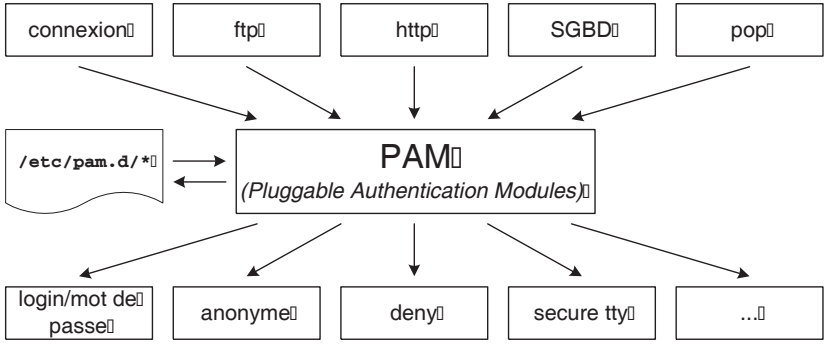


Une telle gestion implique deux inconvénients majeurs :

- Chaque application ayant sa propre méthode d'authentification, il devient rapidement difficile de maintenir un système ayant beaucoup d'utilisateurs devant accéder à un grand nombre de services différents.
- Il n'est pas possible de s'authentifier pour un service autrement qu'en suivant la procédure prévue par le programme.

Le système d'authentification PAM se présente sous la forme d'un ensemble de bibliothèques partagées (ou modules). Ces modules ont chacun leurs propres méthodes d'authentification.

Toute application conçue avec le support de PAM pourra alors utiliser n'importe lequel de ces modules pour authentifier l'utilisateur :



Grâce à cela, l'authentification des applications peut être homogénéisée facilement et adaptée selon les besoins ; la maintenance du système d'authentification s'en trouve facilitée.

De plus, les développeurs qui créent des applications fondées sur ce système n'ont plus à se soucier du type d'authentifications et de l'implémentation dans le code.

a Fichiers de configuration

Il existe normalement un fichier de configuration par application ou service utilisant PAM. Ces fichiers se trouvent dans le répertoire `/etc/pam.d` et portent le nom du service auquel ils sont rattachés.

> *S'il n'y a pas de fichier spécifique pour le service, le fichier `/etc/pam.d/other` fait office de fichier de configuration par défaut.*

La syntaxe d'une ligne d'un fichier de configuration contient trois champs :

```
<type> <stratégie> <chemin et arguments du module>
```

Le premier champ indique le type d'entrées ; les valeurs possibles sont :

auth méthode d'authentification de l'utilisateur, généralement par une demande de login/mot de passe.

account gestion des limites du compte ; par exemple, la mise en place du vieillissement des mots de passe ou la définition de plages horaires pour la connexion.

password modification du mot de passe ; fixe les contraintes liées à la création d'un nouveau mot de passe, comme le nombre minimum de caractères et l'interdiction de mots présents dans un dictionnaire.

session gestion de la session. Le module est activé une fois l'authentification établie pour monter le système de fichiers où se trouve le répertoire personnel de l'utilisateur par exemple.