

Introduction à la sécurité sous Unix

Hervé Schauer

Hervé Schauer Consultants
142 Rue de Rivoli
75039 Paris Cedex 01
Tél: +33 (1) 46 38 89 90
Fax: +33 (1) 46 38 05 05
Herve.Schauer@hsc-sec.fr

1. Unix pas fait pour la sécurité ?

Unix à la réputation d'être un système peu sur. Le prochain numéro de Panoram'X tentera de démystifier le sujet.

La sécurité dépend avant tout de la volonté des utilisateurs de respecter une politique de sécurité, plus que du système d'exploitation lui-même. Unix est un système assez complet vis-à-vis des fonctionnalités de sécurité, qui n'a pas à rougir des autres systèmes, bien au contraire. Il ne manque rien de fondamental à la mise en place d'une politique de sécurité.

Nous allons donc voir brièvement quelques aspects de base de la sécurité sous Unix, parfois oubliés dans les initiations à Unix.

2. La sécurité pas faite pour vous ?

L'importance des systèmes d'information dans le fonctionnement des organisations à l'heure actuelle est croissante. Les pertes dues à la sécurité informatiques sont de plus en plus conséquentes. Ceci montre à quel point il est de plus en plus risqué de ne pas prendre en considération la sécurité informatique.

Il est souhaitable, lors de chaque décision, même benine, que les aspects liés à la sécurité soient pris en compte. Ainsi, petit à petit, la sécurité s'améliorera. On peut aussi analyser les risques que l'on court, et à partir de ces risques mettre en place des parades, mais il faut toujours essayer de garder une vue globale des problèmes, et rechercher le compromis entre les besoins de sécurité et la commodité

d'utilisation du système d'information.

L'important est de ne plus se retrouver avec des problèmes de sécurité simplement dus au fait que l'on y avait pas pensé.

La sécurité est un tout, qui doit être suivie par tous à tous les niveaux, pour l'amélioration du travail de tous.

3. Les Utilisateurs et administrateurs

Les Unix classiques utilisés actuellement proposent deux classes d'utilisateurs : les administrateurs et les autres.

POSIX, à travers les fonctionnalités proposées dans le document P1006.6, en cours de réintégration à l'ISO dans la norme ISO 9945, propose un découpage des privilèges de l'administrateur en un grand nombre de privilèges. Ceci permet de découper le système actuel où l'administrateur (*root*) est tout-puissant, en affectant le minimum de privilèges nécessaires à chaque administrateur ou utilisateur.

Dans le système actuel, il convient de bien distinguer utilisateur et administrateur. En particulier, un utilisateur n'a pas besoin d'être administrateur sur sa station. Certains fournisseurs ont parfois laissé entendre le contraire, mais une informatique distribuée où tout appareil est connecté au système d'information de l'organisation, a besoin d'une administration qui réalise des tâches bien distinctes à l'utilisation de l'outil informatique.

La mise en place d'une administration des machines distincte des utilisateurs permet d'améliorer la sécurité.

Un élément important pour une administration correcte, est que chaque utilisateur doit avoir son propre compte, y compris les administrateurs, qui prendront les privilèges d'administration à l'aide de la commande *su* juste le temps nécessaire.

Un autre élément important pour une administration correcte est que chaque administrateur ait son propre mot de passe d'administration. Cela peut être réalisé simplement, en créant un compte bénéficiant de l'UID 0 qui caractérise l'administrateur, par personne physique réalisant des tâches d'administration. Ceci ne doit pas faire supprimer le compte normal de chaque administrateur, c'est en plus, chaque administrateur a ainsi 2 comptes.

4. Le mot de passe

Sur un système multi-utilisateurs comme Unix, chaque utilisateur, pour travailler, doit s'identifier, grâce au *login*, et s'authentifier, grâce au mot de passe. La réussite de la sécurité demande une politique stricte de choix et de gestion des mots de passe.

L'utilisateur doit bien choisir son mot de passe, en accouplant par exemple deux mots existants avec des chiffres ou des caractères de ponctuation, ou en utilisant des mots écrits en phonétique. Ainsi le mot de passe est simple à retenir par cœur sans jamais avoir besoin d'être noté. Il est aussi important d'apprendre aux utilisateurs à changer leur mot de passe dès qu'ils ont un doute, si quelqu'un aurait pu le voir le taper par exemple.

Bien choisir son mot de passe et bien le gérer sont des éléments clés de la sécurité sous Unix.

5. Contrôle d'accès aux fichiers

5.1 Accès aux fichiers

Le fonctionnement des permissions sous Unix est parfois mal compris par les utilisateurs. Dès qu'un utilisateur a accès à l'interpréteur de commandes ou à un gestionnaire qui lui permet de manipuler ses fichiers, il est souhaitable qu'il ait bien compris le

fonctionnement des permissions. Dans ce cadre, il est préférable de restreindre l'utilisation de la commande *chmod* avec des arguments en octal aux spécialistes, comme *chmod 764*. Pour un utilisateur, il est possible de lui expliquer le fonctionnement avec la notation *augo += rwx* qui est beaucoup plus explicite, qui permet en plus du changement en absolu des modifications relatives des permissions. Les versions POSIX de la commande *chmod* permettent d'écrire *chmod u=rwx,g=rw,o=r*, qui est plus long mais plus compréhensible que *chmod 764*.

5.2 Cas des répertoires

Le fonctionnement particulier des permissions sur les répertoires est aussi important. La distinction entre la permission "r", qui permet de voir la liste des fichiers du répertoire, et la permission "x", qui permet d'aller dans le répertoire et de nommer un fichier de ce répertoire, est à expliquer aux utilisateurs.

De même pour la permission "w" sur le répertoire, qui permet de créer et supprimer un fichier, mais aussi de changer son nom. Celle-ci ne doit pas être confondue avec la permission "w" sur le fichier lui-même, qui permet de changer le contenu du fichier, mais pas d'effacer le fichier.

Une bonne connaissance du fonctionnement des permissions est préférable, afin de profiter de celles-ci sans erreurs, et sans croire à tort que l'on est protégé.

6. Conseils aux utilisateurs

Les utilisateurs doivent connaître quelques éléments :

- Unix étant conçu pour travailler à plusieurs, chaque utilisateur bénéficie d'un répertoire à lui. Il faut conserver ce répertoire protégé des autres afin de protéger ses données.
- La commande *umask*, interne au *shell*, permet de déterminer les permissions associées à chaque fichier lors de leur création. Il est souvent préférable d'avoir un masque donnant le minimum de permissions, comme *umask 077* qui donnera *rwX-----* sur un exécutable ou un répertoire et *rw-----* sur un fichier. Ceci limite l'accès à l'utilisateur propriétaire seulement, tout en lui laissant la possibilité d'utiliser *chmod* pour autoriser d'autres accès.
- De nombreux fichiers dans le répertoire de connexion, visibles avec la commande *ls -la*, doivent impérativement avoir un accès limité au propriétaire, c'est par exemple le cas du fichier ".profile" exécuté lors de chaque connexion (*shell* Bourne ou *shell* conforme à POSIX).
- Les administrateurs ont tous les droits, en particuliers ils peuvent toujours lire les fichiers privés des utilisateurs. La seule protection possible serait de chiffrer les fichiers.
- La sécurité repose sur une bonne administration, tout particulièrement lorsque l'on a un réseau grandissant, il est important d'embaucher et de former des administrateurs compétents.

En suivant et en développant ces quelques éléments, il est possible de mettre en place une bonne sécurité dans les environnements Unix.