Sécuriser l'accès physique à une station Linux*

Lorsqu'une station Linux doit être laissée en libre accès dans un lieu dont on ne contrôle pas totalement les usagers, un certain nombre de précautions doivent être prises pour protéger l'intégrité du système. Nous allons tenter d'établir ici une liste des éléments fondamentaux en terme de sécurité, principalement en ce qui concerne le démarrage du système et la configuration de Lilo.

Depuis la mise sous tension de la machine, jusqu'au moment de la connexion effective d'un utilisateur, il existe toute une chaîne de points d'entrée dans le système. Chaque maillon de cette chaîne de sécurité doit être sérieusement vérifié, car le moindre point faible présente une opportunité d'intrusion illicite.

Avant tout, il nous faut définir le type de dangers contre lesquels nous désirons nous prémunir. Nous supposerons ici que nous risquons d'être confronté à des utilisateurs un peu indélicats, qui essayent de s'introduire dans le système par curiosité plutôt que par réelle volonté de nuire.

Nous nous intéresserons ici à la protection de la station Linux en elle-même, sans traiter par exemples des attaques de pirates provenant d'Internet. La protection d'un système vis-à-vis des tentatives d'effraction provenant du réseau relève d'autres méthodes et d'autres outils.

J'emploie typiquement les mécanismes décrits ici pour protéger des stations installées dans des locaux techniques où de nombreuses personnes sont susceptibles de circuler. L'intégrité physique de la machine n'est pas menacée ; personne ne risque *a priori* d'attaquer le disque dur à coups de maillet. De plus, on suppose que les attaquants éventuels ne sont rien de plus que de simples utilisateurs un peu indélicats ; ils ne sont pas censés par exemple exploiter des failles de sécurité inédites ou récemment découvertes. J'imagine que les mêmes suppositions peuvent être faites pour les machines installées dans des salles d'enseignement.

Mots de passe

Tout d'abord, il faut respecter les principes élémentaires de sécurité, et employer systématiquement des mots de passe corrects sur tous les comptes utilisateurs. L'existence d'un compte utilisateur non-protégé peut être exceptionnellement envisagée dans certaines circonstances. Par exemple, une application spécialisée peut parfois être mise à la disposition de toutes les personnes habilitées à circuler dans le local où se trouve l'ordinateur. Par exemple, un logiciel affichant en permanence les états d'un système industriel doit être accessible à tous les individus accédant à une salle de supervision. Il est alors nécessaire de fournir un compte utilisateur spécifique sans mot de passe démarrant automatiquement l'application. Si dans une telle situation, on tentait d'imposer un mot de passe sur un tel compte, le seul résultat serait de retrouver le mot de passe inscrit sur un *post-it* en haut du moniteur deux jours après l'installation Dans d'autres circonstances (laboratoires, etc.), on peut être amené à créer un compte *guest* permettant à tous de se connecter pour disposer d'un logiciel particulier.

Une règle essentielle reste néanmoins la nécessité de toujours protéger le compte *root* par un mot de passe. Sans même imaginer de malveillance, la moindre maladresse ayant lieu sous cette identité peut avoir des conséquences catastrophiques. Il faut de surcroît comprendre qu'un individu se trouvant face à une machine inconnue, va automatiquement tenter de se connecter sous *root*, avant même d'essayer *guest*, *test*, *free* ceci même sans désir de pirater l'ordinateur, mais simplement parce que c'est le seul compte dont la présence soit à peu près certaine.

Donc, il faut toujours placer un mot de passe sur le compte *root*. Et tant qu'à faire autant un choisir un bon, ce qui signifie rejeter les noms, prénoms, localités ou mots se trouvant dans le dictionnaire. Pas de séries logiques de lettres (`azeaze`), pas d'initiales trop faciles à deviner. Par contre, on peut employer des séquences complexes de chiffres et lettres (`4ew7jnk2`). Si on les juge trop difficile à mémoriser, on peut aussi employer des mots accolés comportant une faute volontaire (`MoDePaçe`), des syllabes ou des lettres remplacées par des chiffres (`L0g1n 6teme`), etc.

Quoiqu'il en soit, nous tenons donc pour acquis que le compte *root* doit être solidement protégé par un mot de passe. Ceci implique également l'utilisation d'un système de *shadow passwords*, pour éviter qu'un utilisateur puisse employer un logiciel d'attaque par force brute pour casser le mot de passe *root*. Le mécanisme des *shadow passwords* est maintenant installé automatiquement avec toutes les distributions Linux courantes.

Protection du démarrage mono-utilisateur

Lorsqu'une station Linux démarre, il est possible, en réponse au message ‘‘ `LILO:` ’’ d'ajouter l'argument ‘‘ `single` ’’ au nom de la partition de démarrage Linux. Ainsi sur la plupart des machines, répondre ‘‘ `linux single` ’’ au

---

* Cet article a été publié dans le numéro 21 (Octobre 2000) de Linux Magazine France.

message ‘‘ `LILO:` ’’ permet d’initialiser le système en mode mono-utilisateur. Ce mode est surtout conçu pour permettre de réparer les maladresses d’administration que l’on a commises en fonctionnement normal. Dès le démarrage, nous pouvons ainsi nous trouver connectés sous l’identité *root* sans avoir besoin de fournir de mot de passe.

Inutile d’insister sur le fait que cette possibilité, pour pratique qu’elle soit dans certaines circonstances, représente néanmoins un fort danger pour une machine que n’importe qui peut relancer (par exemple en effectuant un cycle arrêt / marche en coupant l’alimentation).

Pour éviter ce problème, on peut employer l’option ‘‘ `password` ’’ de Lilo. On édite le fichier `/etc/lilo.conf`, et l’on ajoute une ligne ‘‘ `password=`*`mot_de_passe`* ’’ dans la portion correspondant à l’image Linux à charger. Toutefois cela n’est pas suffisant. À partir de ce moment en effet, Lilo demandera automatiquement le mot de passe au démarrage du système, même dans des conditions normales. Comme la machine doit pouvoir être relancée même en l’absence de l’administrateur *root* (après une coupure électrique par exemple) ce mécanisme est trop contraignant. Il nous faut alors ajouter l’option ‘‘ `restricted` ’’ sur une ligne à la suite de ‘‘ `password=`*`xxx`* ’’, afin que le mot de passe ne soit réclamé que si on essaye d’ajouter un argument à la suite de l’image du noyau à charger (*a fortiori* l’argument ‘‘ `single` ’’).

À nouveau se pose le problème du choix du mot de passe. On peut décider d’utiliser le même que pour le compte *root* (puisque les niveaux de privilèges sont finalement équivalents). Toutefois, cette fois-ci, il convient d’être très prudents lors de la mise en place du mot de passe. Étant donné qu’il est inscrit en clair dans `/etc/lilo.conf`, il faut d’abord s’assurer que ce fichier appartient à *root*, et n’est lisible que par lui :

```
# chown root.root /etc/lilo.conf
# chmod 600 /etc/lilo.conf
```

Ensuite, par acquit de conscience, on peut effacer le mot de passe du fichier `/etc/lilo.conf` une fois qu’on a exécuté `/sbin/lilo`. À ce moment, en effet Lilo aura mémorisé le mot dans ces données de configuration sur le disque, et n’a plus besoin du contenu de son fichier de configuration. J’ai l’habitude en général, une fois exécuté `/sbin/lilo`, de rééditer `/etc/lilo.conf` pour modifier la ligne ‘‘ `password` ’’ ainsi :

```
password = insérez ici le mot de passe root
```

Ce qui présente l’avantage de déclencher un message d’erreur de syntaxe si on essaye de lancer `/sbin/lilo` sans avoir mis à jour le fichier de configuration.

Protection du démarrage sur disquette

Nous avons déjà obtenu qu’il ne soit pas possible d’être automatiquement connecté sous l’identité *root* simplement en ajoutant l’argument ‘‘ `single` ’’ lors du démarrage. Rien n’empêche toutefois un utilisateur mal intentionné de copier une image du noyau sur une disquette, et de créer une arborescence de fichiers minimale sur une autre disquette à la manière des systèmes de dépannage fournis avec certaines distributions. Il lui suffit alors de démarrer la machine sur ces disquettes et de monter ensuite la partition Linux résidant sur le disque dur dans sa propre arborescence. Ayant tous les droits sur cette nouvelle partition, il sera à même d’effacer le mot de passe de *root*, puis de redémarrer la machine.

Pour éviter ceci, il faut s’adresser cette fois-ci au Bios de l’ordinateur. Dans la configuration (*setup*) de la plupart des machines actuelles, il est en effet possible de désactiver la possibilité de démarrage sur disquette – ou de rendre le disque dur plus prioritaire dans l’ordre de démarrage ce qui revient au même. Nous devons toutefois protéger avec un mot de passe la configuration du Bios contre toute modification, sinon notre intrus pourrait réactiver à sa guise le démarrage sur disquette. Naturellement, on peut à nouveau employer le même mot de passe que celui de *root* si on le désire.

La configuration étant en général sauvegardée dans une mémoire protégée par une pile C-Mos, il est possible de l’effacer en retirant la pile, et en court-circuitant les pattes d’alimentation de la mémoire, afin de décharger les condensateurs. Ceci est même parfois expliqué dans la documentation d’utilisation de l’ordinateur. La seule protection possible contre cette intervention est de verrouiller physiquement le capot de l’ordinateur, au moyen d’un cadenas. Rappelons que nous avons considéré que les tentatives d’intrusion que nous désirons couvrir sont motivées par la curiosité ou le goût du défi, mais pas par la volonté de nuire réellement. Si vous craignez que vos visiteurs indésirables attaquent le cadenas à la pince coupe-boulons ou ouvrent le capot de l’ordinateur au pied-de-biche, la seule solution consiste à mettre l’unité centrale hors d’atteinte (ce qui résout par ailleurs tous les autres problèmes de sécurité)

Autres systèmes d’exploitation

Pour l’instant nous n’avons considéré que le cas d’une station comportant uniquement une installation de Linux. Il existe toutefois certaines situations où l’on est obligé de conserver une partition contenant un autre système d’exploitation. Cela peut par exemple être indispensable pour piloter un périphérique non supporté par Linux ou pour utiliser occasionnellement un logiciel n’existant que sur une autre plate-forme (bureautique, application de gestion).

Il faut être conscient que le fait d’offrir un accès Dos par exemple sur la machine représente un risque important en termes de sécurité. En théorie, il faudrait que cet accès soit réservé exclusivement à l’administrateur ou à des utilisateurs de confiance. Ce qui peut être mis en service utilisant l’option ‘‘ `password=`*`xxx`* ’’ de Lilo, dans la section correspondant à l’autre système, sans employer l’option ‘‘ `restricted` ’’ puisque l’on désire limiter la possibilité de démarrer sur cette partition.

Si l’accès Dos doit être inévitablement offert à tous les utilisateurs, une faille de sécurité difficilement réparable apparaît : n’importe qui peut utiliser des outils comme `ext2_tools` ou `fsdext2` pour monter la partition Linux dans un répertoire Dos. Bien que cette partition ne soit utilisable qu’en lecture seule, il devient possible d’accéder au contenu des fichiers comme `/etc/shadow` ou `/etc/lilo.conf` normalement réservés à *root*. Pire, les utilitaires `ltools` permettent de modifier, depuis le Dos, le

contenu d'une partition `ext2`. On peut ainsi effacer le mot de passe crypté de root contenu dans `/etc/shadow`.

Le seul remède consisterait à les placer sur une partition contenant un système de fichiers crypté, comme CFS ou TCFS (*Transparent Crypted File System*), ce qui complique largement la mise en service du système. L'accès Dos présente aussi un autre problème de sécurité, en permettant à n'importe qui d'examiner octet par octet le contenu des secteurs de démarrage du disque dur, où est probablement stocké le mot de passe que Lilo réclame pour l'option `single`.

On évitera donc autant que possible d'autoriser le démarrage d'un autre système d'exploitation.

Conclusion

Nous avons observé comment éviter de laisser sur un système Linux des portes trop faciles à ouvrir. Malgré tout nous ne nous sommes intéressées qu'à l'accès direct à la machine elle-même. Il y a d'autres risques au moins aussi importants :

- Les applications peuvent contenir des erreurs les rendant potentiellement dangereuses. Ceci est essentiellement vrai avec les logiciels installés avec le bit Set-UID *root*. L'administrateur devra rester attentif à toutes les alertes de sécurité annoncées dans certaines listes de diffusion, et appliquer les corrections nécessaires le plus vite possible.

- Si la machine est reliée à un réseau, et à plus forte raison à Internet, les probabilités d'attaques par ce biais sont largement plus importantes. Pour se prémunir – du moins en partie – contre ces risques, il faut suivre les consignes de sécurité habituelles (supprimer les services non utilisés, enregistrer et analyser toutes les tentatives d'intrusion, appliquer les patchs correctifs des applications réseau, etc.)

Si on considère que les tentatives d'intrusion illégales sont limitées, comme nous l'avons fait ici, à des utilisateurs curieux mais pas belliqueux, on peut assurer une surveillance acceptable en examinant régulièrement les fichiers de traces comme `/var/log/messages` ou `/var/log/secure` ainsi qu'en employant la commande last pour rechercher les dernières connexions *root*.

Christophe Blaess < ccb@club-internet.fr>

http://perso.club-internet.fr/ccb/