La sécurité de votre système en 20 points

Stéphane Téletchéa

1. Choisir un mot de passe difficile à trouver, à renouveler

Tout le monde le sait, il ne faut pas utiliser un mot de passe fondé sur un mot du dictionnaire, le nom de son animal de compagnie ou le surnom d'un proche. Un mot de passe difficile à trouver doit contenir au moins 8 caractères, alphabétiques ou non et être difficile à trouver. Ces règles peuvent sembler difficiles à appliquer ou à mettre en pratique, mais prenez plutôt le problème à l'envers : choisissez une phrase que vous pourrez facilement retenir comme « LE Cheval De Henrl IV Etait Blanc », et transformez-la en mot de passe. Transformez les « E » en « 3 », ne conservez que quelques lettres, transformez les « l » en « ! ». En prenant les lettres mises en majuscules, vous avez ainsi le mot de passe « L3CDH!43B », vous pouvez même mélanger minuscules et majuscules pour le rendre encore plus complexe : « L3CdH!43B ». Voilà un mot de passe de 9 caractères facile à mémoriser mais impossible à trouver dans un dictionnaire :-).

Pour plus de sécurité, forcez le changement de mot de passe régulièrement, si votre mot de passe secret venait à être découvert de manière indirecte (via une réutilisation sur un site commercial par exemple), vous aurez une sécurité supplémentaire avec un nouveau mot de passe difficile à trouver.

2. Mettre un mot de passe pour le super-utilisateur root

Ubuntu a choisi de ne pas activer le compte *root* par défaut et de recourir au mécanisme `sudo` pour effectuer toutes les tâches administratives. Il y a cependant des situations, par exemple pour configurer un serveur, où il est plus simple d'avoir un accès *root* total plutôt que de recourir à `sudo`. Pour activer le compte *root*, il suffit de mettre un mot de passe au compte grâce à la commande `sudo passwd root`. Même si vous ne faites pas régulièrement de tâches administratives sur votre machine, c'est une bonne idée de mettre un mot de passe au compte root, au cas où un utilisateur utiliserait un mot de passe faible sur la machine, ou si une faille dans le paquet « sudo » était révélée…

3. Ne jamais lancer l'interface graphique en tant que root

Après avoir activé le compte *root*, il peut être tentant d'utiliser l'interface graphique sous ce profil superutilisateur puisque dans ces conditions, nous nous affranchissons des problèmes de permissions de fichiers, de droits d'accès aux périphériques, etc. Il faut absolument bannir cette pratique car c'est le meilleur moyen d'effectuer une commande dangereuse pour le système sans y prendre garde. Alors qu'un utilisateur lambda ne pourra pas effacer les program-

mes présents dans /usr par exemple, l'utilisateur *root* y aura accès sans difficulté...

4. Supprimer les services non essentiels

Une installation Ubuntu a pour vocation de répondre aux besoins de la plus large base d'utilisateurs possible. Afin d'y répondre au mieux, la configuration par défaut fait donc appel à de nombreux services qui ne vous seront pas forcément utiles pour votre utilisation particulière. Afin d'identifier les services inutiles, vérifiez ceux activés par défaut avec la commande `service --status-all`. Identifiez les services qui ne vous servent pas avec la commande `update-rc.d -f <service> remove` en remplaçant <service> par celui que vous voulez désactiver. Si vous estimez que le service ne vous sera pas ou plus utile, désinstallez le paquet de la distribution, pour enlever une source potentielle d'attaques.

5. Utiliser un pare-feu

Même si votre ordinateur est dans un environnement « sécurisé », il est plus raisonnable d'activer un pare-feu sur les connexions entrantes afin de bloquer les protocoles « intrusifs » qui cherchent à contacter toutes les machines d'un réseau, ce qui est de plus en plus le cas avec les téléphones portables faisant les mises à jour « par les airs ». En regardant les messages enregistrés par le pare-feu, vous vous rendrez certainement compte que de nombreux messages transitent sur votre réseau domestique sans que vous n'y prêtiez garde... Pour activer le pare-feu avec des options prédéfinies, tapez `sudo ufw enable`.

6. Maintenir son système à jour

Même si cela peut parfois paraître fastidieux ou tout le moins gênant, la fréquence des mises à jour et des correctifs de sécurité est un gage rassurant sur un système GNU/Linux. En effet, c'est la force de notre système que de pouvoir répondre rapidement à toute faille identifiée puisque chaque ligne de code peut être auditée et corrigée rapidement. Il serait naïf de croire que les « pirates » ignorent Ubuntu ou toute autre distribution, il existe beaucoup de scripts permettant de tester très rapidement la présence de faille, ce sont les fameux *rootkits*. Maintenir à jour notre système diminue ainsi la possibilité pour un éventuel attaquant de pénétrer notre système.

7. Limiter l'accès physique à la machine et protéger le BIOS

Si vous tenez sérieusement à votre ordinateur et à vos données, limitez l'accès physique à la machine. Mettez un mot de passe dans le bios, mettez un cadenas sur la machine pour empêcher son ouverture et utilisez un câble de sécurité pour qu'il se soit pas volé. Sachez que dès qu'une personne malveillante a un accès physique à votre ordinateur, elle a la possibilité de venir voir le contenu de votre ordinateur sans démarrer le système d'exploitation, par exemple avec un système « Live ». Si le bios a un mot de passe et qu'il ne permet pas de démarrer sur un média amovible (CD-ROM, clé USB, ...), vous ralentissez alors sérieusement l'intrusion de l'utilisateur malveillant.

8. Chiffrer les documents importants

Si certains de vos documents sont sensibles, pensez à les chiffrer. Des solutions logicielles existent, comme par exemple truecrypt. Vous devrez cependant avoir recours à une clé de chiffrement qu'il ne faudra ni perdre ni oublier, au risque de perdre l'accès à vos données. C'est une solution à réserver à vos données les plus précieuses !

9. Installer des paquets issus de dépôts sûrs

L'une des forces de Ubuntu est de pouvoir utiliser de nombreuses sources de paquets via le dépôt « ppa ». Si pour les dépôts les plus connus de la distribution, il y a un contrôle strict du contenu d'un paquet, l'utilisation de dépôts tiers augmente le risque d'installer un paquet corrompu ou qui ne fait pas ce qu'il est censé faire, mais ouvre une porte dérobée sur votre système. N'utilisez que des sources fiables !

10. Limiter l'accès à ses documents les plus sensibles en modifiant leurs permissions

Sans aller jusqu'au chiffrement, il suffit d'enlever les permissions en lecture et écriture à un dossier, à un fichier, pour qu'un autre utilisateur de l'ordinateur n'accède pas à vos données. Cela n'empêchera pas le superutilisateur d'y accéder ou un autre utilisateur ayant les droits `sudo`, mais cela freinera le petit malin qui chercherait, via le réseau, à lire vos documents... Si cet utilisateur malveillant venait à se connecter avec son compte sur votre machine, il ne pourrait ainsi pas lire vos relevés de banque, votre fichier où sont stockés tous vos mots de passe, etc.

11. Être vigilant sur les informations et leur diffusion

L'une des clés pour contourner la sécurité d'un système réside dans l'identification rapide par un « pirate » des failles potentielles du système. La faille la plus évidente et pourtant ignorée, est ce qui s'appelle le « social engineering » ou, en bon français, « tirer les vers du nez ». Cela peut, par exemple, prendre la forme d'un appel téléphonique par lequel un utilisateur se faisant passer pour un employé de votre fournisseur d'accès à Internet vous indique qu'il y a des perturbations sur votre accès Internet (ce qui peut arriver), et qui vous invite à vous rendre sur un site donné. Une fois sur ce site, copie conforme du site réel du fournisseur d'accès, vous entrez vos identifiants en toute bonne foi ; dès lors, la personne qui vous a induit en erreur possède l'accès à toutes vos informations personnelles ! De la même manière, vérifiez toujours quand vous recevez un message qui vous incite à aller sur un site externe qu'il s'agit effectivement de l'adresse du site de destination indiquée dans le message et non d'un lien renvoyant vers une autre page (en général, il suffit de laisser la souris positionnée au-dessus du message pour voir l'adresse du lien).

12. Compléter la configuration du navigateur avec les extensions

L'une des plus grandes menaces pour la sécurité du système vient de sites malveillants dans un contexte où tous les ordinateurs sont reliés en permanence à Internet. Des mises à jour très régulières des navigateurs sont mises en place par les développeurs mais deux précautions valant mieux qu'une, il est parfois utile de bloquer l'exécution de scripts sur certains sites, en ajoutant le greffon « NoScript » sous Mozilla Firefox, par exemple. Idéalement, il faudrait aussi désactiver le greffon « java » lorsqu'il n'est pas strictement nécessaire, à cause des multiples attaques dont il fait l'objet.

13. Installer openssh pour la connexion à distance

Si vous avez besoin de vous connecter à distance avec votre ordinateur, utilisez le couple openssh/openssh-server pour le faire. Dans la mesure du possible, il faut éviter les partages de fichiers sans authentification, même dans un réseau local. Si vos amis viennent vous rendre visite et que vous leur ouvrez l'accès au WiFi pour qu'ils puissent se connecter sur Internet, vous n'aimeriez certainement pas qu'ils se connectent au passage à votre ordinateur via le réseau, sans qu'au moins un mot de passe leur soit demandé…

14. Installer des logiciels de surveillance d'intrusion

Bien qu'un pirate cherchera dans un premier temps à masquer son intrusion dans votre système en modifiant certains binaires pour qu'ils se comportent normalement, il laisse cependant sur votre système quelques traces détectables. Vérifiez l'intégrité des fichiers de votre système avec, par exemple, le logiciel AIDE (*Advanced Intrusion Detection Enviornment*) ou d'autres qui lui sont affiliés comme Tripwire. Vérifiez que votre système est sain ou recherchez la présence de kits de connexion (*rootkits*) grâce au logiciel « chkrootkit » ou encore « rkhunter ». Ces logiciels sont disponibles dans les dépôts officiels de Ubuntu.

15. Vérifier qu'il n'y a pas d'utilisateur exotique sur la machine

Un certain nombre de services ont besoin d'avoir un utilisateur propre, pour des raisons de performance ou de sécurité. La plupart de ces services n'ont pas de « login shell » et ont donc l'entrée */bin/false* ou encore */usr/sbin/nologin* dans le fichier */etc/passwd*. Si vous voyez apparaître un nouvel utilisateur avec un shell de connexion */bin/bash* ou un shell moins courant comme */bin/zsh* par exemple, il faudra vous assurer que vous êtes effectivement à l'origine de cet ajout. Il peut arriver qu'installer un nouveau paquet ajoute un nouvel utilisateur sur votre système, comme l'utilisateur « hplip » si vous installez un imprimante Hewlett-Packard, mais si un nouvel utilisateur apparaît hors de ce cas particulier, il faudra vous méfier.

16. Mettre un mot de passe pour un accès à la base MySQL

La plupart du temps, les administrateurs de la machine, c'est-à-dire vous en règle générale, installent le paquet « mysql-server » en passant vite l'étape de création du mot de passe pour l'utilisateur *root*.

Cela signifie que n'importe qui ayant un accès physique ou à distance à la machine pourra se connecter à la base SQL et regarder les informations qu'elle contient, en faire une copie pour une utilisation ultérieure, ou détruire les données présentes. Suivez la règle de création de mot de passe pour créer un mot de passe spécifique pour *root*, différent de celui du gestionnaire de connexion, et changez-le régulièrement.

17. Cacher la liste des utilisateurs dans le gestionnaire de connexions

S'il est parfois difficile de trouver le mot de passe d'un utilisateur donné, cela devient presque impossible quand l'identifiant de l'utilisateur à usurper est inconnu. Pour cacher le nom des utilisateurs du gestionnaire de connexion (lightdm), il faut ajouter la ligne `greeter-hide-users=true` dans le fichier de configuration */etc/lightdm/lightdm.conf*.

18. Activer le système de sécurité AppArmor

Sur une machine utilisée dans un milieu sensible (exposée sur Internet directement, en libre service, etc.), il est fortement conseillé d'activer le système de sécurité *Application Armor* (AppArmor). Vous contrôlerez ainsi finement les logiciels avec droit d'exécution et les logiciels bloquer. Ce système peut très vite être contraignant de par sa puissance, vous pourrez vous référer à son utilisation plus poussée dans ce magazine pour l'exploiter au mieux.

19. Empêcher le chargement de modules du noyau

Il est arrivé par le passé qu'une faille dans le noyau GNU/Linux permette à un utilisateur lambda de devenir *root* lors du chargement d'un module du noyau par la commande `modprobe`. Dans un cadre normal, sur un système dont la configuration matérielle n'évolue pas, il est tout à fait possible de bloquer ce chargement dynamique de modules dans le noyau. Il suffit de lancer la commande `echo 1 > /proc/sys/kernel/modules_disabled`. Tout chargement de module sera ainsi bloqué, jusqu'au prochain démarrage. Pour rendre la modification permanente, il faudra modifier les réglages du système, ce que vous apprendrez à faire en explorant la page de man idoine : `man sysctl`.

20. Compiler son noyau pour le rendre plus sûr

Pour rendre son système encore plus sûr, il vaut mieux compiler son noyau pour le rendre plus compact, libéré de tous les modules qui ne servent pas au quotidien, et dégagé des problèmes de chargement et déchargement de modules. Tant qu'à le recompiler, vous pourrez aussi en profiter pour lui ajouter le module GrSecurity dont le but est de renforcer encore plus la sécurité du système (*http://en.wikibooks.org/wiki/Grsecurity/Configuring_and_Installing_grsecurity*). En appliquant les règles vues ci-dessus avec un noyau optimisé, votre système deviendra très résistant aux attaques. ■