Sécuriser sa Debian

- Objet : Indications sur la manière de sécuriser une Debian
- Suivi :
  à-compléter
  - Création par smolski le 19/08/2010
  - Testé par Ir0nsh007er le 9/08/2015
- Commentaires sur le forum : C'est ici[1)]

Dicton du jour

> *"Just because you're paranoid doesn't mean they're not after you!"*

« *Ça n'est pas parce que vous êtes paranoïaques qu'ils ne sont pas tous après vous !* »

Vos objectifs

Il n'existe pas de sécurité parfaite, mais une chose est sûre, c'est que plus on veut s'en rapprocher, et plus il faut y consacrer de temps, d'argent, d'efforts et de litres de sueur.
Si vous êtes responsable de la sécurisation d'une machine dans un cadre professionnel, il vous faut bien jauger le rapport temps à allouer / sécurité requise avant de vous lancer dans des opérations chronophages.
Si vous faites cela à titre personnel, qu'est-ce qui relève de la paranoïa et qu'est-ce qui constitue le strict minimum ?

Intégrité des données

- *À quoi servent les sauvegardes ?*
  À récupérer des données qui auraient été effacées de votre ordinateur.
- *À quoi servent ces données ?*
  Cela dépend de chacun de vous, et en fonction de cela, les moyens à mettre en œuvre également.

Prenons quelques cas d'école et les solutions conseillées :

- *J'ai peur de supprimer un fichier important ou de devoir reprendre une ancienne version de celui-ci.*
  Si vos fichiers sont légers (et principalement textuels) un système de suivi de version (VCS) comme git, mercurial ou subversion semble le plus adapté.
  Si vos fichiers sont lourds, les VCS ne sont pas adaptés et des sauvegardes régulières (par exemple sur votre disque dur) sont nécessaires.

- *J'ai peur que mon disque dur lâche.*
  Si vos disques ne contiennent rien d'autres qu'une Debian configurée sans données personnelles (comme dans un cyber-café), alors enregistrez juste la configuration sur un autre

disque.
Sinon, en fonction de vos besoins, vous pouvez programmer une sauvegarde régulière sur un autre disque (chaque mois, chaque semaine, chaque jour, chaque heure, ...).
Si vous ne voulez vraiment rien perdre, mettez en place un RAID-1,5 ou 6.

- *J'ai peur de perdre tous mes disques durs en même temps (orage, vol, perte...).*
  Dans ce cas, effectuez des sauvegardes sur un support externe
- *J'ai peur de perdre mon disque de sauvegarde en même temps (cambriolage, incendie, inondation...).*
  Dans ce cas, faites une sauvegarde via internet sur un serveur situé ailleurs (OVH, Online, autres...).
- *J'ai peur qu'une catastrophe d'ampleur mondiale efface mon disque dur (EMP naturel ou non).*
  Dans ce cas, rangez une de vos sauvegardes externes dans une cage de Faraday, ou gravez vos données dans du marbre.
- *J'ai peur qu'un astéroïde vienne s'écraser sur mes plaquettes de marbre.*
  Embarquez vos données dans un satellite du système solaire.
- *J'ai peur que le soleil se transforme en supernova et détruise mes satellites.*
  Oui, moi aussi...

Sauvegarder, restaurer, archiver ses données

- Sauvegarder, Restaurer, Archiver Vos données et votre système seront vite récupérés.

Confidentialité des données

Données présentes sur votre ordinateur

- Est-ce grave si quelqu'un d'autre arrive à accéder à vos données ?
- À quel prix voulez-vous l'empêcher ?
- Contre quel type d'attaque voulez-vous vous préparer ?

- J'ai peur que l'on vole mon disque dur / qu'on le récupère quand je le jette / que telle organisation secrète (d'état ou non) m'oblige à lui donner mon disque dur
  - Chiffrez vos données avec cryptsetup / truecrypt
  - Sachez que la loi peut vous obliger à donner les mots de passe protégeant vos archives (à moins que vous ne les ayiez oubliés...)

- J'ai peur que quelqu'un pirate mon ordinateur
  - Limitez le nombre de services accessibles depuis l'extérieur, en coupant les serveurs et en mettant en place un pare-feu (voir ufw et iptables).
  - Éliminez tout service avec authentification en clair (FTP, POP3, IMAP, webmail HTTP, login HTTP)
  - Tenez-vous à jour des mises à jour de sécurité, voir le manuel apt
  - Utilisez des mots de passe forts et différents, sur votre ordinateur pour les sessions utilisateurs et la session root avec l'aide de Sécurité passwd - libpam-pwquality voire aussi en plus sur chacun des services web que vous utilisez avec un outil tel que keepassx.

Pour des raisons de sécurité, il est recommandé de ne jamais utiliser deux fois le même mot de passe. En effet, si un des comptes se trouve compromis, alors tous les comptes utilisant ce mot de passe le sont.

Comme il est difficile de se souvenir de 100 mots de passe forts complètement différents, il existe des logiciels pour faire cela.

Firefox, Icedove / Thunderbird et d'autres logiciels proposent de mémoriser les mots de passe pour vous. Il est en règle général dangereux de confier la gestion des mots de passe à un logiciel chargé de faire autre chose. En particulier, des failles dans Firefox permettaient dans le passé de récupérer les mots de passe enregistrés.

Donc au lieu de cela, il est préférable d'utiliser un logiciel spécialisé, comme Keepassx

- J'ai encore peur (données très sensibles)
  - Stockez vos données sur une machine qui n'est pas directement accessible depuis l'extérieur
  - Ne gardez pas de copie en clair de vos données.
- J'ai toujours peur (données vitales)
  - Ne connectez pas votre ordinateur à internet

Attention, chiffrer votre disque dur et faire des sauvegardes en clair, c'est un peu idiot.

Données échangées

Le protocole SMTP et tel que les données sont en général envoyées en clair entre les différents serveurs. Cela fait d'ailleurs le bonheur de Google et des FAI et autres personnes mal intentionnées qui prennent beaucoup de soin à lire attentivement chacun de vos emails (via des scripts, pas avec des petits lutins sans papier exploités dans la cave) afin de faire des études statistiques anonymes sur vous, vos habitudes, vos produits achetés, la difficulté de vos mots de passe, etc.

Vous en aurez déduit que quand un site vous envoi votre mot de passe par mail, vous êtes bon pour le changé, un ou deux robots l'ont déjà lu.

Une autre des faiblesses de SMTP fait qu'il n'y a pas d'authentification (ou plutôt, peu, et pas toujours utilisée). Une des solutions pour palier à ces deux défauts est le chiffrement et la signature de son courrier via un outil tel GPG.

Authenticité, identité et confidentialité Pour vous protéger de tout cela, vous pouvez envoyer des messages chiffrés (personne à part votre destinataire ne peut les déchiffrer) ou/et signés (votre destinataire peut vérifier que vous seul avez pu l'envoyer et l'avez envoyé tel quel).

Un des systèmes permettant de réaliser ce chiffrement est GPG.

Il existe différentes interfaces entre GPG et différents clients de courriel.

- Enigmail est une extension pour icedove / Thunderbird (existe aussi pour

Windows)
- mutt est configurable pour utiliser directement GPG

Attention,

- **si vous chiffrez vos mails mais donnez la clé de chiffrement à votre hébergeur (et que vous n'êtes pas votre propre hébergeur)**
- **si vous chiffrez vos mails mais ne protégez pas votre boîte mail par un mot de passe fort et unique**
- **si vous envoyez par un biais non chiffré le mot de passe de votre boîte mail**

dans ce cas vous faites les choses de travers et votre chiffrement était un peu inutile.

Communications entre différents ordinateurs reliés par internet

Lorsque plusieurs ordinateurs sont en réseau à l'intérieur d'une infrastructure, vous pouvez supposer que personne de l'extérieur ne pourra venir écouter ce qui se passe sur le réseau depuis l'intérieur, à moins qu'il trouve une brèche dans une des passerelles de ce réseau vers internet.

Si les ordinateurs en réseau ne sont pas tous dans un même local mais sont reliés uniquement via Internet, il est alors intéressant de créer des canaux de communication sécurisés que l'on appelle des réseaux privés virtuels.

- vpn

À noter : le protocole ssh permet des échanges sécurisés, en particulier le partage de fichiers avec sshfs.

Attention, plus un réseau à de points d'entrée et plus il est exposé à un attaquant.

Détection d'intrusion

Comment savoir si votre machine subit des attaques, a été piraté ou même s'il y a encore une backdoor dessus ?

IDS : Systèmes de détection d'intrusion

Pour surveiller les attaques.

- Snort Le programme snort est considéré comme sniffers, mais il a aussi la fonction de IDS (Intrusion Detection System = détecteur d'intrusion).
- logcheck

Recherche heuristique de rootkits

Détecter une intrusion après coup par les traces qu'elle laisse.

- Chkrootkit. Il permet de détecter les traces d'une attaque et de rechercher la présence d'un rootkit.
- Rkhunter. Il permet de détecter la présence de rootkits, portes dérobées et exploits.

Se protéger contre les attaques

- Configurer son pare-feu pour se protéger des attaques (D)DoS
- Configurer son pare-feu pour bannir automatiquement les machines tentant une attaque par bruteforce
- Configurer son pare-feu pour bannir automatiquement les machines tentant un scan des ports
- Configurer son pare-feu pour cacher les ports ouverts par port-knocking
- Filtrer les mails reçus, avant de les distribuer à vos utilisateurs de Windows, avec un antivirus

Quelques moyens

- iptables, une interface permettant de configurer le filtrage des paquets par le noyau Linux
- ufw, un pare-feu pour configurer simplement les règles iptables, et son interface graphique gufw
- shorewall, le configurateur de pare-feu et passerelle
- Clamav, un antivirus pour protéger les copains qui sont pas sous Linux. Les pôv…

L'aspect humain

Avoir un mot de passe solide, c'est bien. Mais si c'est pour le donner au premier site de phishing venu, ça n'est pas la peine.

C'est pourquoi il est très important d'éduquer tous les utilisateurs d'un serveur sur les risques de phishing et autres arnaques.

L'idée est la suivante, et c'est un cas d'école puisque c'est ce qui est arrivé à TheOnion :

1. Je veux pénétrer un réseau, plutôt que de bruteforcer tous les mots de passes possibles, je vais simplement les demander aux utilisateurs.
2. Je crée une page qui ressemble trait pour trait à la page de changement de mot de passe du service
3. J'envoie un mail aux utilisateurs (mais pas au staff) leur demandant de changer leur mot de passe. Pour qu'ils ne se doutent de rien en voyant l'url, je la camoufle en html [url=http://url2/]http://url1[/url] où url2 est une adresse sur terrain apparemment neutre (google) redirigeant vers url3 où se trouve la fausse page de changement de mot de passe.
4. Sur les x utilisateurs, il y en a un qui tombe dans le panneau et donne son mot de passe.
5. Je crée ensuite une page qui ressemble à une page de connexion au compte
6. J'envoie un lien au staff depuis le compte compromis indiquant « euh, faudrait revoir cet article » avec un lien pointant vers la fausse page de connexion au compte (protégé par la même astuce que tout à l'heure).
7. Un des membres du staff croit que cette demande d'identifiants est légitime pour accéder à l'article cité.

8. En fait non et je récupère les identifiants du membre du staff.

Autre astuce :

1. Je fais une page de fishing pour un site à la noix où je sais que l'utilisateur à un compte
2. Je teste le mot de passe donné sur ce site sur son compte mail principal
3. Ça marche, j'ai son compte mail et donc virtuellement quasiment tous ses mots de passe... (coucou paypal, ebay et autres numéros de cartes pré-enregistrés)

Attention, ces astuces ne sont pas là pour vous transformer en pirates du dimanche, mais pour vous montrer combien c'est facile et ça marche... Donc soyez prudents !

Gestion des services

Un utilisateur système sans mot de passe (au sens « pas de mot de passe valide », pas au sens « avec un mot de passe vide »), n'est pas une surface d'attaque.

La surface d'attaque, c'est le service qui tourne, et en particulier le service qui écoute sur un port.

Tu peux lister les processus en train d'écouter sur un port via

```
ss -pltn
```

Pour chacun d'eux, tu peux consulter la page man si elle existe, pour avoir une idée du rôle du programme.

Exemple :

```
man rpcbind
```

savoir d'où il provient avec dpkg :

```
dpkg -S rpcbind
```

Et une fois que tu as repéré le paquet, avoir plus d'info sur la fonction générale du paquet avec show :

```
apt show rpcbind
```

Si tu ne comprends pas à quoi sert le paquet, ou que tu n'es pas sûr d'en avoir besoin, tu peux faire semblant de l'enlever en ajoutant dans la commande de suppression remove l'option `-s` ainsi :

```
apt -s remove rpcbind
```

Et là, tu regardes les paquets qu'il veut t'enlever.

1. Si ce sont des paquets dont tu n'as pas besoin, alors tu peux y aller sans trop de risque en enlevant tout ça.

2. À l'inverse, si c'est un paquet vital qui s'en va, ça veut dire que le service en question est important pour celui-ci et donc pour ton utilisation.

Lien vers le Forum

https://debian-facile.org/viewtopic.php?pid=313960#p313960

Liens divers

- Les malwares - Généralités
- Les logiciels malveillants sous Linux
- Devenez parano et chiffrer tout avec GnuPG
- Apg, un générateur de mot de passe en ligne de commande, simple et efficace
- Cpm, un (autre) générateur de mot de passe en ligne de commande, simple et efficace
- Les virus - Bouh !
- Outils et règles de sécurité, sur privacytools.io (anglais)
- Contrôle parental : la sécurité, c'est aussi protéger les plus jeunes du world "wild" web

[1)]

N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !