Les bases

de la sécurisation

du système

Sommaire

Introduction.

Ce n'est pas parce que le système Gnu Linux est réputé sécurisé qu'il n'y a pas à s'en préoccuper. Un système est sécurisé si on le sécurise. Si on n'y prend pas garde, Gnu Linux ou pas, il y aura des failles.

Il y a différentes techniques et logiciels à utiliser pour rendre son système plus sûr, nous en verrons ici les bases.

La sécurité du système est un enjeu de plus en plus important, puisque nous faisons et stockons de plus en plus de choses avec notre ordinateur, et que personne n'est à l'abri d'une attaque.

Il faut donc bien comprendre la sécurité d'un système informatique, et s'en préoccuper sérieusement si on ne veut pas se faire voler ses données (même si pour un particulier le risque est quand même faible).

Voici un petit article intéressant sur la sécurité d'un ordinateur sous Windows :

http://bugbrother.blog.lemonde.fr/2009/02/20/la-duree-de-vie-dun-ordinateur-non-protege-est-de-4-minutes/

Présentation de la sécurité informatique.

Le système d'information représente les données, les ressources, les logiciels et le matériel informatique.

Assurer sa sécurité consiste à garantir plusieurs objectifs :

l'intégrité des données : est-ce bien nos données, n'ont-elles pas été modifiées, corrompus ?

la confidentialité : n'autoriser l'accès à certaines données qu'aux personnes ayant les droits nécessaires.

la disponibilité : s'assurer que le système fonctionne et est toujours accessible.

la non répudiation : une fois une action faite, on ne doit pas pouvoir la nier, ni même l'attribuer à un autre utilisateur.

l'authentification : chaque utilisateur doit être authentifié pour accéder aux ressources.

Il faut établir une politique de sécurité, en étudiant les besoins, les risques potentiels, en surveillant les vulnérabilités du système, et en préparant quoi faire en cas d'attaque ou de compromission.

La sécurité informatique est quelque chose de global, où il faut prendre en compte un certain nombre de facteurs : la sécurité physique des machines, les dangers liés au réseau, le niveau de sensibilisation du personnel utilisant ses ressources, les besoins du personnel, les données à traiter.

Bien sûr, pour un particulier, les choses sont beaucoup plus simples. Nous allons voir ici comment rendre plus sûr son système Gnu Linux, afin d'être mieux protéger face à un éventuel pirate informatique.

Les bases.

Pour commencer, il faut que le système soit toujours à jour. On peut le configurer (pour Mageia dans le Centre de Contrôle) afin qu'il recherche automatiquement et régulièrement les mises à jour disponibles. Elles ne font pas que proposer de nouvelles fonctionnalités, elles corrigent également d'éventuelles failles dans le système. Donc, c'est important d'avoir un système et ses logiciels mis à jour très régulièrement.

Ensuite, il faut, si cela est nécessaire, désactiver le compte invité.

Il faut éviter d'utiliser la connexion automatique de votre utilisateur, on est jamais à l'abri d'un vol.

Utiliser des mots de passe forts, sans mot du dictionnaire, nom, prénom ou même date de naissance. Il faut des majuscules, des minuscules, des chiffres ainsi que des caractères spéciaux. Et il doit être assez long (au moins 8 ou 10 caractères).

On peut mettre un mot de passe au niveau du BIOS (Basic Input Output System) afin d'empêcher quelqu'un de modifier sa configuration, et on peut faire de même avec Grub, le chargeur de démarrage du système, afin qu'un attaquant ne puisse pas le modifier pour tenter de démarrer autre chose.

Pensez à vérifier que le bureau à distance est désactivé.

Ne pas se connecter en root sur le système, mais plutôt utiliser la commande *sudo* si l'on a besoin de faire des modifications.

Sécuriser sa configuration.

Il faut modifier le umask par défaut. Cette commande gère les droits d'accès, en octal, par défaut lorsque l'on crée un fichier ou un dossier, et se configure dans le fichier */etc/profile*. Il est en général défini à *022*, ce qui correspond à : *rw- r-- r--* lecture (r) pour le propriétaire, écriture (w) pour le groupe et pour tous. Pour plus de sécurité, on peut le mettre à *027* ou même à *077*.

Vérifier que votre système utilise les mots de passe shadow, qui permettent de stocker les mots de passe de façon bien plus sécurisé. Regardez dans le fichier */etc/passwd* (qui est lisible par tous les utilisateurs du système), et si le deuxième champ contient un « x », cela veut dire que le mot de passe se trouve dans le fichier */etc/shadow* et qu'il est crypté. De plus, ce fichier n'est lisible que par l'administrateur, et ne contient pas d'informations sur l'utilisateur.

Exemple de fichier passwd, les champs sont séparés par des « : », le premier étant le login, le second le mot de passe :

root:x:0:0:root:/root:/bin/bash

bin:x:1:1:bin:/bin:/bin/sh

daemon:x:2:2:daemon:/sbin:/bin/sh

Exemple de fichier shadow :

root:$2a$08$/BMjDxLPSGJZyoJQQMbHlOK5uA5rWwdlS4DtPcbrcS:15580:0:99999:7:::

bin::15580:0:99999:7:::*

daemon::15580:0:99999:7:::*

Il faut vérifier qu'il n'y a pas de comptes sans mot de passe, à l'aide d'une des deux commandes suivantes :

grep -v ':x:' /etc/passwd

awk -F: '($2 == "") {print}' /etc/shadow

Ensuite, on peut désinstaller les programmes dont on ne se sert pas. Moins il y a de programmes, moins il y a de risques.

Même chose pour les services, certains sont tout à fait inutile, et il vaut mieux les désinstaller (avez-vous besoin du bluetooth, de cups, samba..?).

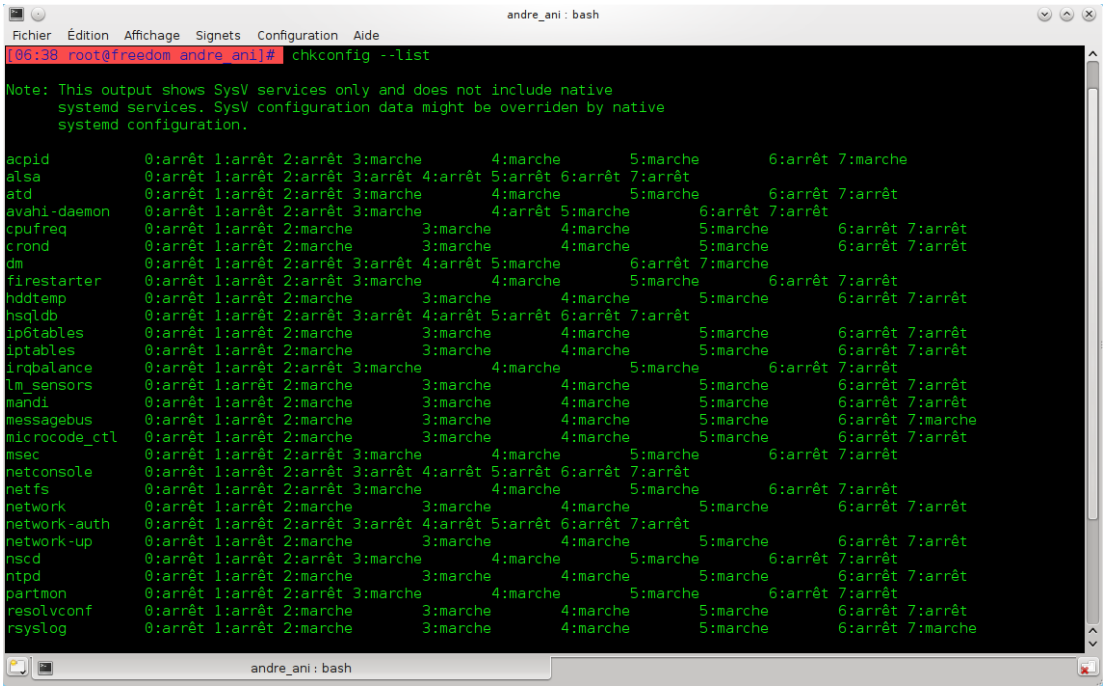
Voici une liste des services :

http://www.hscripts.com/tutorials/linux-services/list.php

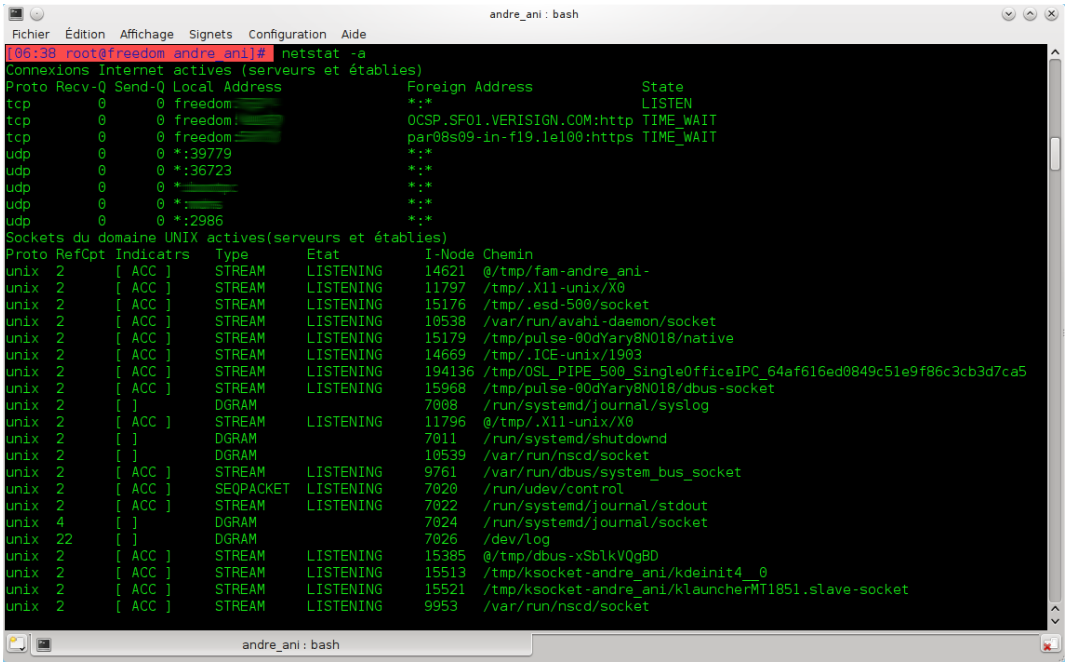
Pour vérifier les services actifs, on peut le faire en ligne de commande avec *chkconfig* (en root) ou avec le Centre de Contrôle de Mageia. Pour désactiver un service sur les run-level 3 et 5, faites :

chkconfig --level 35 service off

Faites *chkconfig –list*, en root, pour voir tous les services actifs suivant les run-level :

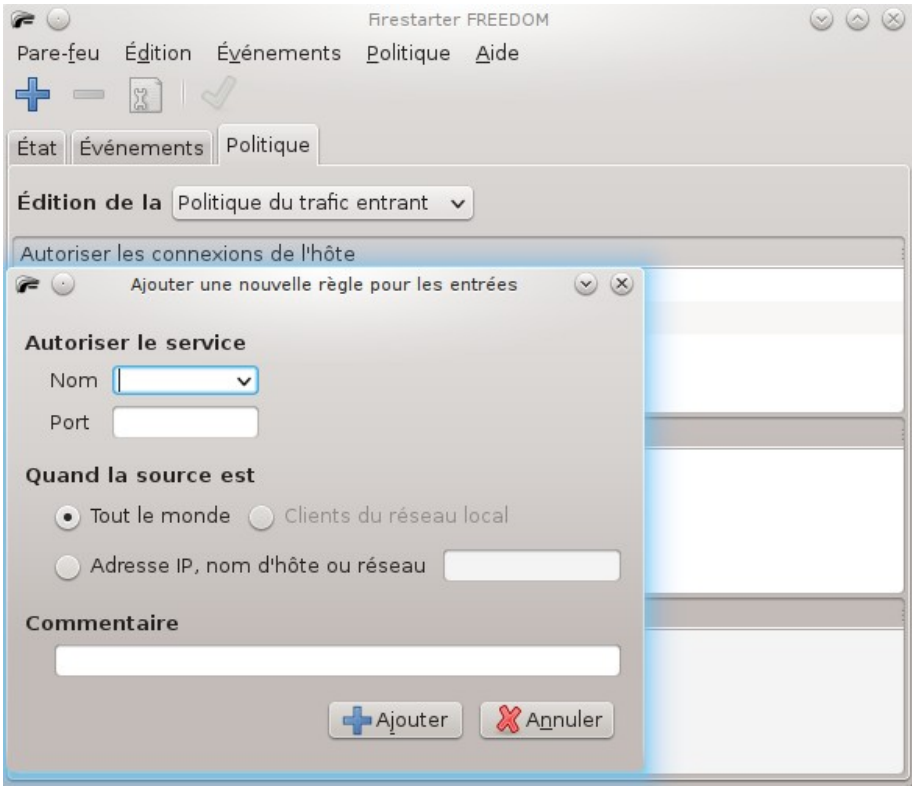


Autre chose à vérifier, les ports ouverts sur votre machine, qui sont des portes d'entrée pour des pirates, à l'aide de la commande *netstat -a* :



Voici une liste des ports pour savoir à quoi ils correspondent https://fr.wikipedia.org/wiki/Liste_de_ports_logiciels

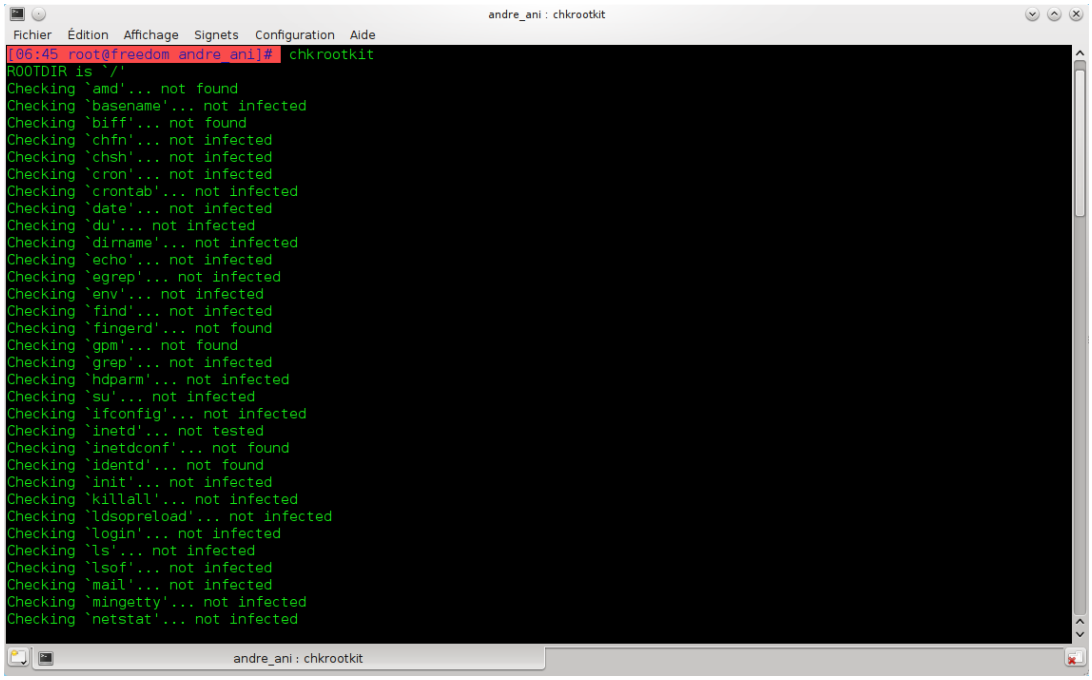
Une fois la vérification faite, à l'aide d'un firewall, comme Firestarter par exemple, n'autorisez que les services dont vous avez besoin.



Se protéger.

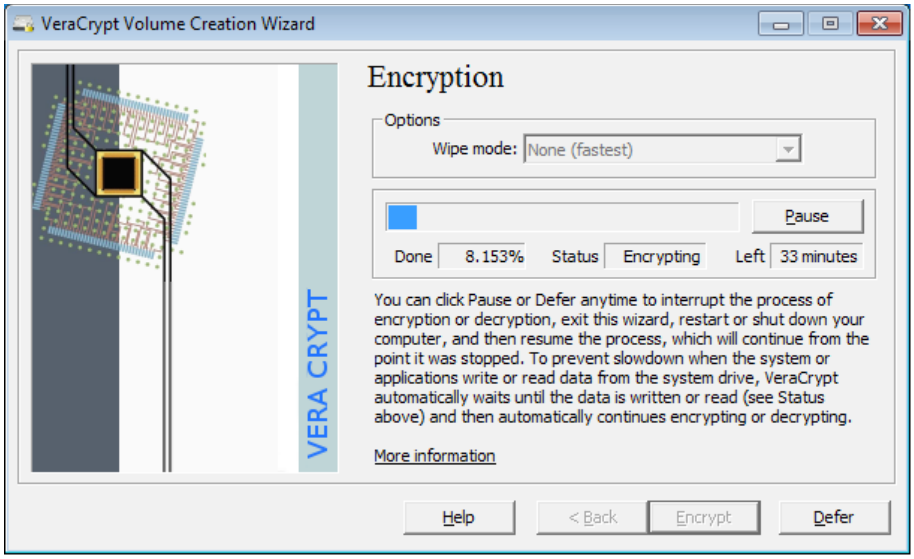
Un *rootkit* est un logiciel malveillant, furtif, qui tente de donner accès au compte root à un utilisateur n'ayant pas les droits nécessaires. Pour s'en protéger, il existe deux principaux logiciels à installer (et à utiliser régulièrement), qui sont *RkHunter* et *ChkRootkit*.

Voici *ChkRootkit*, qui s'utilise en ligne de commande (comme *RkHunter*) :



Il faut aussi penser au chiffrement de ses données sensibles (fichiers, dossiers), à l'aide de GnuPG (sous KDE l'interface graphique est KGPG http://utils.kde.org/projects/kgpg/), Ecryptfs, ou même de ses partitions, grâce à VeraCrypt, que vous pouvez télécharger depuis le site officiel :

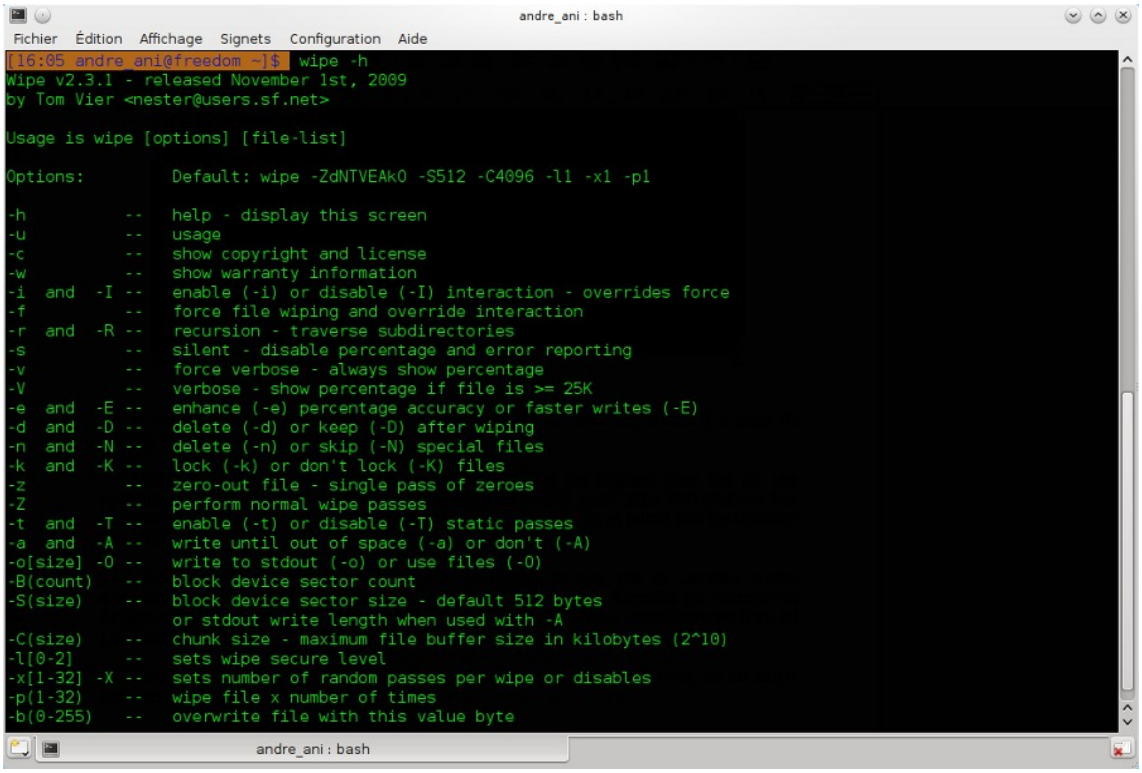
https://veracrypt.codeplex.com/



L'effacement sécurisé de ses données est également à ne pas négliger, pour être sûr que personne ne puisse récupérer des données que l'on pensait ne plus avoir. *Wipe* écrit plusieurs fois des données aléatoires par dessus les fichiers à supprimer, afin que l'on ne puisse plus les retrouver ni les lire.

Par exemple, cette commande effacera le dossier ainsi que ses sous-dossiers en écrivant 35 fois par dessus :

wipe -r -i -Q 35 -q dossier



Chose importante à faire, la vérification de ses fichiers de logs, afin de surveiller si rien d'anormal ne se passe. Les fichiers de logs se trouvent dans */var/log*. Regardez par exemple les fichiers *messages* ou *user.log*. Le système inscrit dans ces fichiers tout ce qui se passe, du démarrage à l'extinction, que se soit un problème matériel, une erreur d'un logiciel ou une tentative raté de connexion. Il existe des logiciels pour faciliter la surveillance des logs, tel *LogWatch (http://sourceforge.net/projects/logwatch/?source=navbar)* par exemple.

Dernière chose, faites très régulièrement des sauvegardes de toutes vos données (vos favoris internet, votre carnet d'adresses, vos photos et autres documents), sur un disque dur externe, une clé USB ou un DVD. On est jamais à l'abri d'une panne matériel, d'une surtension ou d'un vol.

Le mieux est d'utiliser un CD ou un DVD, on ne peut pas écrire directement dessus et cela améliore donc l'intégrité des données. Pensez à vérifier vos sauvegardes également.

Durcissement du système.

Pour aller encore plus loin dans la sécurisation du système, il existe de nombreuses techniques de configuration que l'on peut mettre en place. Mais ce cours n'est qu'une introduction à la sécurité.

Voilà quelques liens pour les plus curieux (ou les plus paranoïaques) :

Sur le site de l'agence nationale de la sécurité des systèmes d'informations

http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/systeme-d-exploitation-linux/recommandations-de-securite-relatives-a-un-systeme-gnu-linux.html

Basé sur la distribution Debian :

http://www.debian.org/doc/manuals/securing-debian-howto/ap-harden-step.fr.html

En anglais :

http://cromwell-intl.com/security/linux-hardening.html

http://www.cyberciti.biz/tips/linux-security.html

http://www.puschitz.com/SecuringLinux.shtml

Il existe également des logiciels permettant de durcir Gnu Linux, afin de le rendre encore plus sûr. On peut nommer les plus importants qui sont :

SELinux : https://fr.wikipedia.org/wiki/SELinux

AppArmor : https://fr.wikipedia.org/wiki/AppArmor

Bastille Unix : https://fr.wikipedia.org/wiki/Bastille_UNIX

Plus utilisé pour des réseaux, mais pas seulement, on peut également utiliser un IDS (Intrusion Detection System). Ces logiciels permettent de détecter si un hôte a été compromis par un pirate, ou infecté par un virus. Il en existe 3 types différents, les IDS réseaux, les IDS machines, et les hybrides.

https://fr.wikipedia.org/wiki/Système_de_détection_d'intrusion

Le plus utilisé est Snort : http://www.snort.org/

Pour finir.

La sécurité informatique est quelque chose de complexe, car il y a de nombreux points à prendre en considération. Pour un particulier, cela est plus simple. Même si un système peut être conçu de manière très sécurisé, si l'utilisateur ne fait pas attention à son utilisation, il y aura tout de même des failles.

Gnu Linux est bien conçu, de façon plus sécurisé que certains concurrents (les droits d'utilisateurs avancés, le compte root, le système de fichier journalisé) mais on peut toujours améliorer la sécurité de son système, et c'est une préoccupation de tous les instants.

Si vous avez bien suivi ce cours, et si vous mettez en pratique ce que vous y avez appris, vous aurez nettement réduit les risques de piratage et votre système sera plus sûr.

Bibliographie.

https://fr.wikipedia.org/wiki/Sécurité_des_systèmes_d'information
https://fr.wikipedia.org/wiki/Sécurité_des_données
http://www.commentcamarche.net/contents/secu/secuintro.php3
http://uselinux.over-blog.fr/article-securite-et-linux-partie-1-75676323.html
http://www.debian.org/doc/manuals/securing-debian-howto/index.fr.html#contents
http://www.inetdoc.net/guides/tutoriel-secu/index.html
http://doc.ubuntu-fr.org/securite
http://www.tldp.org/HOWTO/Security-HOWTO/
http://www.linuxsecurity.com/docs/colsfaq.html
http://www.linuxsecurity.com/content/section/9/161/