|  |  |  |
| --- | --- | --- |
|  | Durcissement d’un serveur Linux | |
| **Table des matières**  [Introduction 3](#_Toc79496940)  [Contrôles de sécurité 4](#_Toc79496941)  [Chiffrement 6](#_Toc79496942)  [Chiffrement des communications des données 6](#_Toc79496943)  [Services 6](#_Toc79496944)  [Suppression des services FTP, Telnet et rlogin/rsh 6](#_Toc79496945)  [Suppression des logiciels ou applications inutiles 7](#_Toc79496946)  [Un service réseau par système 7](#_Toc79496947)  [Noyau Linux 7](#_Toc79496948)  [Noyau Linux et les logiciels à jour 7](#_Toc79496949)  [Sécurité 8](#_Toc79496950)  [Extensions de sécurité Linux 8](#_Toc79496951)  [SELinux 8](#_Toc79496952)  [Utilisateurs et groupes 8](#_Toc79496953)  [Comptes d'utilisateurs Linux et politique de mot de passe fort 8](#_Toc79496954)  [Renforcement de la protection par mot de passe 9](#_Toc79496955)  [Configuration du vieillissement des mots de passe 10](#_Toc79496956)  [Verrouillage des comptes d'utilisateurs après échecs de connexion 11](#_Toc79496957)  [Vérifier qu'aucun compte n'a de mot de passe vide 11](#_Toc79496958)  [Aucun compte non root ne possède un UID défini sur 0 11](#_Toc79496959)  [Désactivation de la connexion root 11](#_Toc79496960)  [Sécurité physique du serveur 12](#_Toc79496961)  [Autres mesures 12](#_Toc79496962)  [Définir le mot de passe du BIOS 12](#_Toc79496963)  [Définir le mot de passe du chargeur de démarrage GRUB 12](#_Toc79496964)  [Délai de configuration pour les interpréteurs de commande (shells) de connexion 13](#_Toc79496965)  [Configuration du verrouillage de l'écran 13](#_Toc79496966)  [Désactivation de CTRL + ALT +SUPP 13](#_Toc79496967)  [Sécurité du centre de données 13](#_Toc79496968)  [Ports réseau en écoute 14](#_Toc79496969)  [Suppression de X Window (X11) 14](#_Toc79496970)  [Configuration du pare-feu basé sur Iptables et TCPWrappers 15](#_Toc79496971)  [Renforcement du noyau (/etc/sysctl.conf) 15](#_Toc79496972)  [Renforcement de la sécurité du noyau avec sysctl 15](#_Toc79496973)  [Paramètres du noyau 15](#_Toc79496974)  [Modification d’un paramètre 17](#_Toc79496975)  [Emplacements /proc/sys 19](#_Toc79496976)  [Partitions de disque 19](#_Toc79496977)  [Point de montage systemd 20](#_Toc79496978)  [Quotas de disque 20](#_Toc79496979)  [Désactivation du protocole IPv6 21](#_Toc79496980)  [Désactivation des binaires SUID et SGID indésirables 21](#_Toc79496981)  [Fichiers modifiables par tout les utilisateurs 22](#_Toc79496982)  [Identification des fichiers orphelins 22](#_Toc79496983)  [Utilisation d’un service d'authentification centralisé 22](#_Toc79496984)  [Kerberos 22](#_Toc79496985)  [Journalisation et audit 23](#_Toc79496986)  [Impression des messages du tampon en anneau (*buffer ring*) du noyau Linux 24](#_Toc79496987)  [Commande journalctl (systemd) 24](#_Toc79496988)  [Rotation des journaux 26](#_Toc79496989)  [Utilitaires Logwatch et Logcheck 27](#_Toc79496990)  [Audition du système avec auditd 27](#_Toc79496991)  [Sécuriser le service openSSH 28](#_Toc79496992)  [Système de détection/prévention d'intrusion 28](#_Toc79496993)  [Désactivation des périphériques USB/Firewire/Thunderbolt 29](#_Toc79496994)  [Pilote de stockage USB 29](#_Toc79496995)  [Liste noire 29](#_Toc79496996)  [Option BIOS 30](#_Toc79496997)  [Chiffrement du disque dur 30](#_Toc79496998)  [Option du GRUB 30](#_Toc79496999)  [Fail2ban comme IDS 30](#_Toc79497000)  [Installation de fail2ban 30](#_Toc79497001)  [Protection des fichiers, des répertoires et des disques 31](#_Toc79497002)  [Sauvegardes 31](#_Toc79497003)  [Autres recommandations 31](#_Toc79497004) | |  |

# Introduction

C'est une tâche compliquée, ardue et longue, même pour les administrateurs système chevronnés, de savoir ce qu'est un **ensemble raisonnable de paramètres de sécurité pour n'importe quel système d'exploitation**.

Le durcissement d’un serveur Linux est le processus visant à rendre un système plus sûr.   
**Après leur installation**, les **serveurs Linux ne sont pas durcis** (avec une surface d'attaque minimisée).

C'est le travail de l’administrateur système se préparer à chaque éventualité et de **mettre en place des systèmes pour s’informer de toute activité suspecte à l'avenir**.

À un niveau élevé, dès qu'un appareil, comme un **serveur**, est dans le **domaine public** - c'est-à-dire visible du monde extérieur - il devient une **cible pour les pirates (*hackers*)**. Un système non sécurisé est un **terrain de jeu pour les hackers qui souhaitent accéder aux données ou utiliser le serveur comme autre nœud pour leurs attaques DDOS** à grande échelle.

Le pire, c'est que sans une bonne sécurité, **on ne saura peut-être jamais si le serveur a été compromis**.   
Un pirate informatique peut avoir obtenu un accès non autorisé au serveur et copié les données sans rien modifier. Le serveur a peut-être fait partie d'une attaque DDOS et on ne le saura pas.   
On peut constater un bon nombre des violations de données à grande échelle dans l'actualité - les entreprises ne découvrent souvent la fuite ou l'intrusion de données que longtemps après le départ des pirates.

Contrairement à la croyance populaire, les pirates informatiques ne veulent pas toujours modifier quelque chose ou usurper des données pour de l'argent.   
Ils souhaitent parfois simplement copier les données sur un serveur pour leurs entrepôts de données (il y a beaucoup d'argent dans les mégadonnées) ou pour utiliser secrètement le serveur à des fins néfastes.

Le durcissement d’un serveur Linux n'est donc pas un processus simple.

Voici quelques règles générales qui suivent les meilleures pratiques courantes ...

* Utiliser uniquement les **commandes è l’aide de sudo** ;
* Ne **jamais configurer un serveur pour qu'il s'exécute en tant que root**   
  (sauf pour le temps d'initialisation)   
  et s’assurer de quitter tous les privilèges inutiles avant d'accepter les demandes ;
* Sécuriser au mieux le **pare-feu et interdire tout accès inutile** ;
* Ne pas **installer pas de logiciels inutiles ou instables**.

Durcir un système Linux implique une **bonne connaissance modèle CIA** ...

* **Confidentialité**  
  Les information*s* sensibles ne doivent être accessibles qu'à un ensemble d'individus prédéfinis.   
  La transmission et l'utilisation non autorisées des informations doivent être restreintes.   
  Par exemple, la confidentialité des informations doit garantir que les informations personnelles ou financières d'un client ne sont pas obtenues par une personne non autorisée à des fins malveillantes telles que le vol d'identité ou la fraude de crédit ;
* **Intégrité**  
  Les **informations ne doivent pas être modifiées de manière à les rendre incomplètes ou incorrectes**.   
  Les utilisateurs non autorisés ne devraient pas avoir la possibilité de modifier ou de détruire des informations sensibles ;
* **Disponibilité**  
  Les **informations doivent être accessibles aux utilisateurs autorisés à tout moment où elles sont nécessaires**.   
  La disponibilité est une garantie que les informations peuvent être obtenues avec une fréquence et une disponibilité convenues.   
  Ceci est souvent **mesuré en termes de pourcentages** et identifié formellement dans les **accords de niveau de service** (SLA) utilisés par les fournisseurs de services réseau et leurs entreprises clientes.

# Contrôles de sécurité

La sécurité informatique est souvent divisée en **trois catégories principales distinctes**, communément appelées contrôles ...

* **Physique**
* **Technique**
* **Administratif**

Ces trois grandes catégories définissent les **principaux objectifs d'une mise en œuvre appropriée** **de la sécurité**.   
Au sein de ces contrôles se trouvent des sous**-catégories qui détaillent davantage les contrôles** et la **manière de les mettre en œuvre**.

**Contrôles physiques**  
Le contrôle physique est la mise en œuvre de mesures de sécurité dans une structure définie **utilisée pour décourager ou empêcher l'accès non autorisé à du matériel sensible**.

Quelques exemples de contrôles physiques ...

* **Caméras de surveillance** en circuit fermé ;
* **Systèmes d'alarme de mouvement** ou **thermique** ;
* **Gardes de sécurité** ;
* **Portes en acier verrouillées** et à **pêne dormant** ;
* **Biométrie**   
  (comprend les empreintes digitales, la voix, le visage, l'iris, l'écriture manuscrite et d'autres méthodes automatisées utilisées pour reconnaître les individus) ;
* ...

**Contrôles techniques**Les contrôles techniques utilisent la **technologie comme base pour contrôler l'accès et l'utilisation des données sensibles** dans une structure physique et sur un réseau.

Les contrôles techniques ont une portée considérable et englobent des technologies telles que ...

* **Chiffrement** ;
* **Carte à puce** ;
* **Authentification réseau** ;
* **Listes de contrôle d'accès** (ACL) ;
* **Logiciel d'audit de l'intégrité des fichiers** ;
* ...

**Contrôles administratifs**  
Les contrôles administratifs définissent les **facteurs humains de sécurité**.   
Ils **impliquent tous les niveaux de personnel au sein d'une organisation** et déterminent quels **utilisateurs ont accès à quelles ressources** et informations par des moyens tels que …

* **Formation et sensibilisation** ;
* **Plans de préparation aux catastrophes** et de **reprise d'activité** ;
* **Stratégies de recrutement** et de **séparation du personnel** ;
* ...

Voici ce qui est un point de départ.  
Il y a encore beaucoup à faire ...

Sécuriser un serveur Linux est important afin de **protéger ses données**, sa **propriété intellectuelle** et son **temps contre les pirates informatiques**.   
L'**administrateur** **système est responsable de la sécurité** d’un hôte Linux.

Conseils de sécurité et liste de contrôle pour le renforcement des serveurs Linux

# Chiffrement

## Chiffrement des communications des données

Toutes les données transmises sur un réseau sont ouvertes à la surveillance.   
Il est important de **chiffrer les données transmises dans la mesure du possible** avec un mot de passe ou à l'aide de clés/certificats.

Pour les transferts de fichiers, on préfèrera utiliser les **utilitaires scp, ssh, rsync ou sftp**.   
Il est également possible de monter le système de fichiers du serveur distant ou son propre répertoire personnel à l'aide d'**outils spéciaux SSHFS et FUSE**.

**GnuPG** permet de **chiffrer et de signer ses données et communications** car il dispose d'un système de gestion de clés polyvalent ainsi que de modules d'accès pour toutes sortes de répertoires de clés publiques.

**OpenVPN** est un **VPN SSL léger et économique**.   
Une autre option consiste à essayer est l’**utilitaire Tinc** qui utilise la **mise en tunnel et le chiffrement** afin de créer un réseau privé sécurisé entre des hôtes sur Internet ou un réseau local privé non sécurisé.

# Services

## Suppression des services FTP, Telnet et rlogin/rsh

Dans la plupart des configurations réseau, les **noms d'utilisateur**, les **mots de passe**, les **commandes FTP**, **telnet**, **rsh** et les **fichiers transférés peuvent être capturés** par n'importe qui sur le même réseau à l'aide d'un renifleur de paquets tel que **Wireshark**.

La solution à ce problème consiste à utiliser **OpenSSH** , **SFTP** ou **FTPS** (FTP sur SSL), qui **ajoute le chiffrement SSL ou TLS** à FTP.

Pour **supprimer NIS, rsh et autres services obsolètes** …  
>> **sudo apt --purge remove xinetd nis yp-tools tftpd atftpd tftpd-hpa telnetd rsh-server rsh-redone-server**

|  |  |
| --- | --- |
|  | La plupart de ces utilitaires ne sont pas installés par défaut sur une station de la famille Debian ou de la famille RHEL. |

## Suppression des logiciels ou applications inutiles

On doit éviter d'installer des logiciels inutiles pour **diminuer le nombre de vulnérabilités logicielles**.

Les gestionnaires de paquets RPM (rpm, zypper, yum et dnf) ou DEB (dpkg, APT et aptitude) permettent d’examiner tous les ensembles de paquets logiciels installés sur un système.

On doit supprimer tous les paquets indésirables …  
**>>** **sudo yum|dnf list installed  
>>** **sudo yum|dnf remove <Nom du paquet>**

**>>** **sudo dpkg --list  
>>** **sudo dpkg --info <Nom du paquet>  
>>** **sudo apt remove <Nom du paquet> --purge  
>>** **sudo apt purge <Nom du paquet>  
>>** **sudo apt autoremove**

**>>** **sudo zypper se --installed-only  
>>** **sudo zypper info <Nom du paquet>  
>>** **sudo zypper remove <Nom du paquet>**

## Un service réseau par système

Il est préférable d’exécuter les **différents services réseau** sur …

* des serveurs ;
* une instance de machines virtuelles   
  ou
* de conteneurs distincts.

Cette bonne pratique **limite le nombre d'autres services qui peuvent être compromis**.   
Par exemple, si un attaquant parvient à exploiter un logiciel tel qu'Apache flow, il obtiendra un accès à l'intégralité du serveur, y compris à d'autres services tels que MySQL/MariaDB/PGSql, le serveur de messagerie, ...

Une autre bonne pratique est **d’utiliser un utilitaire de conteneurisation**   
(LXC, Docker, Podman, Proton, …).

# Noyau Linux

## Noyau Linux et les logiciels à jour

L'**application** **de correctifs de sécurité** est une partie importante de la maintenance du serveur Linux.

Linux fournit tous les outils nécessaires pour **maintenir un système à jour** et permet également des **mises à niveau faciles entre les versions**.

**Toutes les mises à jour de sécurité doivent être examinées et appliquées** dès que possible.

Encore une fois, on utilise le gestionnaire de paquets afin d’appliquer toutes les mises à jour de sécurité …  
**>> sudo yum|dnf uodate  
>>** **sudo apt update && sudo apt upgrade && sudo apt autoremove**  
**>>** **sudo zypper update**

* Il est possible de configurer un système compatible RHEL pour qu’il envoie une notification de **mise à jour effectuée par yum|dnf par courriel** ;
* Une autre option consiste à **appliquer toutes les mises à jour de sécurité à l'aide d’une tâche cron** ;
* Pour les distributions Debian et dérivés, il est **possible d’utiliser apticron pour envoyer des notifications** de sécurité.   
  Il est également possible de configurer des **mises à niveau sans surveillance** pour un serveur …  
  >> **sudo apt install unattended-upgrades apt-listchanges bsd-mailx**

# Sécurité

## Extensions de sécurité Linux

Linux est livré avec divers correctifs de sécurité qui peuvent être utilisés pour se prémunir contre les programmes mal configurés ou compromis.

Si cela est possible, on doit utiliser **SELinux et d'autres extensions de sécurité Linux** afin d’appliquer des limitations sur le réseau et d'autres programmes.   
Par exemple, **SELinux fournit une variété de politiques de sécurité pour le noyau Linux**.

### SELinux

Il est fortement recommandé d'utiliser SELinux qui **fournit un contrôle d'accès obligatoire** (MAC ou *Mandatory Access Control*) **flexible**.

Dans le cadre du **contrôle d'accès discrétionnaire** (DAC ou *Discretionary Access Control*) **Linux standard**, une application ou un processus exécuté en tant qu'utilisateur (UID ou SUID) **dispose des autorisations de l'utilisateur sur des objets** tels que des **fichiers**, des **sockets** et d'autres **processus**.

L'exécution d'un noyau **MAC protège le système contre les applications malveillantes ou défectueuses** qui peuvent endommager ou détruire le système.

# Utilisateurs et groupes

## Comptes d'utilisateurs Linux et politique de mot de passe fort

La mise en œuvre d'une politique de mot de passe fort est un **aspect important de la protection d'un serveur** contre les cyberattaques et les violations de données. Certaines **bonnes pratiques pour les stratégies de mot de passe** incluent l'application d'une **longueur minimale** et la **spécification de l'âge du mot de passe**.

Il faut s’assurer d'avoir une **bonne et forte politique de mot de passe**.   
Par exemple, un bon mot de passe comprend…

* **au moins 12 caractères** ;
* **un mélange de lettres** ;
* **de chiffres** ;
* **de caractères spéciaux** ;
* **...**

Parmi les éléments des plus importants, le **choix d’un mot de passe dont on se souviendra**.   
On peut utiliser des outils tels que *John the ripper* afin de découvrir les mots de passe des utilisateurs faibles sur un serveur.

Les **commandes useradd/usermod** permettent de créer et gérer des comptes d'utilisateurs.

## Renforcement de la protection par mot de passe

Pour Debian et dérivés …  
Installation du paquet libpam-cracklib …  
**>>** **sudo apt install libpam-cracklib**

|  |  |
| --- | --- |
|  | Pour ce qui suit … Pour Debian et dérivés, le fichier à modifier sera /etc/pam.d/common-password ou /etc/security/pwquality.conf ; Pour les autres distribution, le fichier à modifier sera /etc/pam.d/system-auth ou /etc/security/pwquality.conf. |

Pour **exiger une longueur du mot de passe** …  
On accède au fichier désiré ;  
On modifie la longueur minimale de caractères de tous les mots de passe en modifiant la   
**directive minlen=12**   
(avec le nombre de caractères souhaité).

Pour **empêcher la réutilisation du mot de passe** …  
On **accède au fichier désiré** ;  
On **ajoute la directive remember=x**.  
Par exemple, si on souhaite empêcher un utilisateur de réutiliser l'un de ses cinq derniers mots de passe …  
**remember=5**.

Pour **appliquer les spécifications des caractères** …  
On accède au fichier désiré ;  
On modifie les directives …

* **lcredit** (minuscules) ;  
  **ucredit** (majuscules) ;   
  **dcredit** (chiffres)   
  et   
  **ocredit** (autres caractères).

Ces quatre paramètres permettent d’appliquer les spécifications de caractères dans les mots de passe.  
Par exemple, si on veut exiger que les mots de passe contiennent un de chaque paramètre, on peut modifier …  
**lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1**

|  |  |
| --- | --- |
|  | La **directivve Enforce\_for\_root** garantit que, même si c'est l'utilisateur **root qui définit le mot de passe, les stratégies de complexité doivent être appliquées**. |

Pour **appliquer l'âge du mot de passe** …  
On recherche les directives suivantes dans le **fichier /etc/login.defs** et on les **modifie par la durée (jours) de son choix**.

Par exemple …  
**PASS\_MIN\_AGE : 3  
PASS\_MAX\_AGE : 90  
PASS\_WARN\_AGE : 14**

## Configuration du vieillissement des mots de passe

La **commande chage permet de modifier le nombre de jours** entre les changements de mot de passe et la **date du dernier changement de mot de passe**.

Ces informations sont utilisées par le système pour déterminer le moment où un utilisateur doit changer son mot de passe.   
Le **fichier /etc/login.defs définit la configuration spécifique** pour la suite de mots de passe fantômes, y compris la **configuration du vieillissement des mots de passe**.

Pour **désactiver le vieillissement du mot de passe** ...  
**>>** **sudo chage -M 99999 <Nom Utilisateur**>

Pour **obtenir les informations d'expiration du mot de passe** …  
>> **sudo chage -l <Nom Utilisateur>**

Enfin, on peut également **modifier le fichier /etc/shadow** …  
**{Nom Utilisateur}:{Mot de passe}:{Dernière modification du mot de passe}:{Nombre minimum de jours}:{Nombre maximum de jour}:{Avertissement}:{Compte Inactif}:{Date d’expiration}:  
{userName}:{password}:{lastpasswdchanged}:{Minimum\_days}:{Maximum\_days}:{Warn}:{Inactive}:{Expire}** …  
où ...

**Minimum\_days  
Nombre minimum de jours requis** **entre les changements de mot de passe**, c'est-à-dire le nombre de jours restants avant que l'utilisateur ne soit autorisé à modifier son mot de passe ;

**Maximum\_days**  
**Nombre maximal de jours pendant lesquels le mot de passe est valide**   
(après quoi l'utilisateur est obligé de changer son mot de passe) ;

**Warn**  
**Nombre de jours avant l'expiration du mot de passe avant que l'utilisateur soit averti** que son mot de passe doit être modifié

**Expire**  
**Nombre de jours depuis le 1er janvier 1970** (epoch) pendant lesquels le **compte est désactivé**, c'est-à-dire une date absolue spécifiant quand la connexion ne peut plus être utilisée.

**Recommandation** …  
**>>** **sudo chage -M 60 -m 7 -W 7 <Nom Utilisateur>**

## Verrouillage des comptes d'utilisateurs après échecs de connexion

Sous Linux, il est possible d’utiliser la **commande faillog pour afficher les enregistrements de l’utilitaire faillog** ou pour **définir des limites d'échec de connexion**.

L’utilitaire faillog permet de form**ater le contenu du journal des échecs à partir du fichier de journalisation /var/log/faillog**.   
Il peut également être utilisé pour **maintenir les compteurs d'échecs et les limites**.

Pour voir les tentatives de connexion infructueuses …  
**>> faillog**

Pour déverrouiller un compte après des échecs de connexion …  
**>> faillog -r -u <Nom Utilisateur>**

**Remarque** …  
Il est aussi possible d’utiliser la **commande passwd pour verrouiller et déverrouiller des comptes utilisateurs**.  
Pour verrouiller un compte …  
**>> passwd -l <Nom Utilisateur>**

Pour déverrouiller un compte …  
**>>** **passwd -u <Nom Utilisateur>**

## Vérifier qu'aucun compte n'a de mot de passe vide

La **commande awk** permet d’identifier les utilisateurs dont le **mot de passe est vide** …  
**>> sudo awk -F: '($2 == "") {print}' /etc/shadow**

Il est alors possible de verrouiller les comptes fautifs …  
**>>** **sudo passwd -l <Nom Utilisateur>**

## Aucun compte non root ne possède un UID défini sur 0

Seul le **compte root doit posséder l'UID 0** avec des **autorisations complètes** pour accéder au système.   
La **commande awk** permet d’afficher tous les comptes dont l'**UID est** **défini** **sur** **0** …  
**>>** **sudo** **awk -F: '($3 == "0") {print}' /etc/passwd**

On ne devrait voir que la ligne suivante …  
**root:x:0:0:root:/root:/bin/bash**

Si d'**autres** **lignes sont affichées**, il faut les **supprimer ou s’assurer que d'autres comptes sont autorisés** à utiliser l'UID 0.

## Désactivation de la connexion root

On **ne doit jamais se connecter en tant qu'utilisateur root**.

On devrait **privilégier l’utilisation de sudo** pour exécuter des commandes au niveau root en cas de besoin.   
**sudo améliore considérablement la sécurité** du système **sans partager le mot de passe root** avec d'autres utilisateurs et administrateurs.

sudo fournit également des **fonctionnalités d'audit et de suivi simples**.

Cette pratique ne fait toutefois pas l’unanimité chez les administrateurs système.  
Selon certains, Debian n’est pas prévu pour être utilisé sans root. Cela peut éventuellement poser problème.  
Pour d’autres, par souci de sécurité, on doit le désactiver s’il s’agit d’un serveur web qui aura une grande visibilité.  
Autrement …

* **PermitRootLogin à no** dans sshd\_config  
  Ne pas oublier d’**ajouter** **un utilisateur dans le groupe sudo** ;
* **Modifier le port 22** pour un port plus exotique afin d’éviter la plupart des balayages ;
* **Ajouter un utilisateur comme auth user** pour que ce dernier puisse ouvrir une session en SSH ;
* **Mettre en place fail2ban** ;
* **Ajouter une règle iptables** pour n’**autoriser que** **certaines adresses IP**.

# **Sécurité phys**ique du serveur

On doit **protéger l'accès à la console physique** des serveurs Linux.   
On peut **configurer le BIOS et désactiver le démarrage à partir de périphériques externes** tels que de des cédéroms ou des clés USB.

On peut définir le **mot de passe du BIOS** **et du** **chargeur de démarrage GRUB** afin de protéger ces paramètres.

Toutes les salles **de serveurs doivent être verrouillées** et toutes les personnes doivent passer une sorte de **contrôle de sécurité avant d'accéder** à une salle de serveurs.

# Autres mesures

### Définir le mot de passe du BIOS

Le BIOS/UEFI est un microprogramme (*firmware*) de démarrage, conçu pour être le **premier code** **exécuté par un PC lorsqu'il est allumé**.   
Il contrôle **de nombreux paramètres système importants**, y compris les **périphériques** **à partir desquels le système essaiera de démarrer** et dans **quel ordre**.

Il est intéressant d’**attribuer un mot de passe** afin d'**empêcher toute** **modification** **non** **autorisée** de la configuration du BIOS/UEFI.

### Définir le mot de passe du chargeur de démarrage GRUB

Par défaut, la plupart des distributions Linux modernes utilisent GR**UB comme chargeur de démarrage par défaut**.

GRUB peut être utilisé pour **sélectionner parmi différentes images de noyau disponibles** sur les partitions d'un système d'exploitation particulier, ainsi que pour **transmettre des paramètres de démarrage aux noyaux**.   
Il permet également de **démarrer à partir de différentes partitions ou supports**.

GRUB peut être utilisé pour **contourner toutes les mesures de sécurité** (y compris l'authentification) en utilisant le **mode mono-utilisateur**.   
On doit **protéger GRUB par mot de passe contre la modification des paramètres de démarrage** et pour **améliorer la sécurité du serveur**.

### Délai de configuration pour les interpréteurs de commande (shells) de connexion

On peut configurer n'importe quel système Linux pour **déconnecter automatiquement les utilisateurs après une période d'inactivité**.

Pour ce faire on doit créer un **fichier nommé /etc/profile.d/autologout.sh** …  
**>>** **sudo nano /etc/profile.d/autologout.sh**

On y ajoute les directives suivantes …  
**TMOUT=300  
readonly TMOUT  
export TMOUT**On enregistre le fichier et on ferme le fichier.

On **définit ensuite les autorisations** …  
**>>** **sudo chmod +x /etc/profile.d/autologout.sh**

Ce **script implémente un délai d'inactivité de 5 minutes** pour l’interpréteur de commandes /bin/bash.

### Configuration du verrouillage de l'écran

Lorsqu’un **utilisateur quitte temporairement l'écran de la console**, l'écran de verrouillage doit être déployé pour **empêcher les passants d’utiliser le compte**.   
Il est important **de former tous les utilisateurs à verrouiller l'écran** lorsqu'ils doivent quitter la console.

Il existe **plusieurs façons de verrouiller un serveur** ou **un bureau Linux**.

Le **programme vlock** (l'un des nombreux programmes pour verrouiller l'écran) verrouille une ou plusieurs sessions sur la console.   
vlock peut **verrouiller le terminal actuel** (local ou distant) ou l'**ensemble** **du système de console** **virtuelle**, ce qui désactive complètement tout accès à la console.

### Désactivation de CTRL + ALT +SUPP

Toute personne ayant un accès physique au clavier d’un serveur peut simplement utiliser la **combinaison de touches CTRL + ALT + SUPP pour redémarrer le serveur** sans avoir à se connecter.

Pour **désactiver cette fonctionnalité** …  
**>>sudo systemctl mask ctrl-alt-del.target  
Created symlink /etc/systemd/system/ctrl-alt-del.target → /dev/null.  
>>** **sudo systemctl daemon-reload**

## Sécurité du centre de données

Ces astuces **n'empêcheront pas quelqu'un de démarrer le serveur** à partir d'un autre support.   
Un **attaquant déterminé démarrerait simplement dans un autre environnement**, écraserait l'enregistrement de démarrage principal, monterait ou copierait les volumes physiques, détruirait les données ou tout ce qu'il peut imaginer. Il est donc essentiel de **restreindre l'accès à la salle des serveurs et de verrouiller le BIOS avec un mot de passe**.

Il est **impossible de protéger complètement un système contre un attaquant disposant d'un accès physique**, c'est pourquoi la **sécurisation de l'espace** dans lequel se trouve le système doit être considérée comme une **étape nécessaire**.

La **sécurité physique joue également un rôle important pour les centres de données**. L'accès physique au site est généralement **limité au personnel sélectionné**.   
La **surveillance par vidéo** et des **agents de sécurité permanents** sont presque toujours présents si le centre de données est grand ou contient des informations sensibles sur l'un des systèmes qu'il contient.   
Afin d'accéder au centre de données, tous les **invités doivent franchir des barrières** **d'authentification à deux facteurs**.   
Il est préférable d’utiliser des camé**ras sensibles au mouvement** dans toutes les installations pour suivre toutes les activités du centre de données.

## Ports réseau en écoute

La **commande ss est un outil utilisé pour afficher des informations relatives aux sockets réseau** sur un système Linux. L'outil affiche des **informations plus détaillées que la commande netstat** qui est utilisée pour afficher les connexions socket actives.

La **commande ss affiche des statistiques pour le protocole TCP** (Transmission Control Protocol), le **protocole UDP** (User Datagram Protocol), Unix (interprocessus) et les **sockets bruts**.

Les **sockets bruts fonctionnent au niveau Réseau du modèle OSI**.   
Les messages ICMP (Internet Control Message Protocol) et l'utilitaire ping utilisent tous deux des sockets bruts.

**Remarque** …  
La **commande netstat est maintenant obsolète** et **ne fait plus l’objet de développement**.  
Elle a été **remplacée par la commande ss**.  
Toutefois la commande netstat demeure la plus utilisée car la **commande ss n’a pas d’équivalent sous Windows**.

**Remarque** …  
Comme alternative, on peut toujours utiliser l’utilitaire nmap …  
**>> nmap -sT -O <Nom du serveur>  
>>** **nmap -sT -O localhost**

Pour plus d’information, voir le document complémentaire.

## Suppression de X Window (X11)

Les fonctionnalités offertes par X Window sur un serveur ne sont pas requis.   
Il n'y a aucune raison d'exécuter X11 sur un serveur de messagerie dédiée ou d'un serveur Web Apache/Nginx.   
Il suffit d’utiliser le service SSH.  
Il est donc préférable de désactiver et supprimer X Windows afin d’améliorer la sécurité et les performances du serveur.

Pour supprimer tous les bureaux (cela prendra un certain temps) …  
**>>** **sudo apt remove --auto-remove --purge libx11-.\***

Ensuite, on installe deborphan pour supprimer les fichiers orphelins …  
**>> sudo apt install deborphan**

Pour afficher les paquets devenus orphelins...  
**>>** **sudo deborphan -sz**

Ensuite, on supprime tous les fichiers orphelins...  
**>>** **sudo apt remove --purge $(deborphan)**

Enfin, on supprime les pacquets inutiles qui ne sont pas orphelins...  
**>>>** **sudo apt-get autoremove**

## Configuration du pare-feu basé sur Iptables et TCPWrappers

iptables est un programme applicatif de l'espace utilisateur qui permet de configurer le pare-feu (Netfilter) fourni par le noyau Linux.   
On utilise un pare-feu pour filtrer le trafic et autoriser uniquement celui qui est nécessaire.

On peut également utiliser les TCPWrappers, un système d’ACL (*Access Control List*) réseau basé sur l'hôte afin de filtrer l'accès réseau à Internet.   
Il est possible d’empêcher de nombreuses attaques par déni de service à l'aide d'iptables.

## Renforcement du noyau (/etc/sysctl.conf)

Le **fichier /etc/sysctl.conf est utilisé pour configurer les paramètres du noyau** lors de son exécution.   
Linux lit et applique les **paramètres de /etc/sysctl.conf** au démarrage.

Avec /etc/sysctl.conf, on peut configurer divers paramètres réseau et système Linux tels que …

* Limitation de la configuration transmise par le réseau pour IPv4 ;
* Limitation de la configuration transmise par le réseau pour IPv6 ;
* Activation de la protection execshield ;
* Prévention contre l’attaque par inondation syn (syn flood) commune ;
* Activation de la vérification de l'adresse IP source ;
* Diminution de l’impact d’une attaque d'usurpation contre l'adresse IP du serveur ;
* Enregistrement de plusieurs types de paquets suspects, tels que les paquets falsifiés, les paquets acheminés par la source et les redirections.

### Renforcement de la sécurité du noyau avec sysctl

sysctl est un **utilitaire en ligne de commandes** pour **modifier les paramètres du noyau** Linux.  
Des **paramètres et options sont disponibles** afin d'**activer** **des composants du noyau**.  
sysctl permet de modifier ces paramètres.

Les **paramètres disponibles sont ceux listés sous /proc/sys/**.

Pour **afficher les valeurs actuelles** …  
**>> sudo sysctl -a**ou **>> sudo sysctl --all**  
**>> sudo sysctl -A  
>> sudo sysctl net.ipv4.conf.all.rp\_filter  
>> sudo sysctl -a --pattern 'net.ipv4.conf.(eth|wlan)0.arp'**

Pour **modifier ces paramètres** …  
**>>** **sudo sysctl -a**

### Paramètres du noyau

Sous la **structure de répertoires /proc/sys** se trouvent des fichiers permettant de **modifier le comportement du noyau**. Certains de ces fichiers concernent des **périphériques de stockage**, tels que des lecteurs SCSI, des lecteurs SATA/IDE et des cédéroms.   
Les **modifications apportées à ces fichiers modifient les paramètres du noyau**, ce qui entraîne un comportement différent des périphériques de stockage.

En d'autres termes, **systctl permet de modifier les paramètres du noyau stockés dans /proc/sys**.

**>> cat /proc/sys/dev/cdrom/lock   
1**

Un **fichier doit contenir une valeur de 0 ou 1**, essentiellement une **valeur booléenne vrai ou faux**.

Lorsque la **valeur de ce fichier est 1**, le **lecteur de cédérom est verrouillé** lorsqu'un cédérom est monté.   
C’est pourquoi **on ne peut pas éjecter un cédérom** sur un système Linux en appuyant sur le bouton d’éjection du lecteur. Si cette **valeur est définie sur 0**, le **noyau déverrouille le lecteur de cédérom** et on peut éjecter un cédérom, même s'il est monté.

En règle générale, une **valeur de 1 est préférable** car on ne souhaite pas supprimer un périphérique actuellement monté, mais il peut être **pratique de désactiver cette fonctionnalité**.

Un exemple …  
Le **paramètre réseau /proc/sys/net/ipv4/ip\_forward** **autorise**, **ou non**, le **transfert de paquets entre interfaces réseaux**.  
Ce dernier peut avoir **deux états** ...

* **0** --> **non actif**
* **1** --> **actif**

C'est donc un **paramètre de type booléen**.

Toutefois, il est aussi **possible d'avoir des valeurs**, par exemple **/proc/sys/net/ipv4/route/min\_pmtu** retourne une **valeur 512** que l'on peut modifier.

### Modification d’un paramètre

Linux propose **trois méthodes pour définir de nouvelles valeurs** pour des paramètres de noyau donnés

* **Définition de la valeur à l’aide de procfs**  
  On utilise la commande echo pour écrire des données dans des variables (changement temporaire) …  
  **>> sudo echo <Valeur> > /proc/sys/<Répertoire>/<Variable> ;**
* **Définition temporaire à l’aie de la ligne de commande**On utilise la commande sysctl avec l'option -w …  
  **>> sudo sysctl -w <Variable> = <Valeur> ;**
* **Modification du fichier de configuration /etc/sysctl.conf** (définition permanente)  
  On commence par accéder au fichier /etc/sysctl.conf ;  
  On ajoute par la suite …  
  **<Variable> = <Valeur>**Pour charger les nouveaux paramètres, on entre la commande …  
  **>> sudo sysctl -p**   
  ou  
  **>>** **sysctl -p /etc/sysctl.conf**C'est habituellement la méthode recommandée.

La **dernière méthode modifiera les paramètres de façon permanente** **au démarrage** à partir du fichier /etc/sysctl.conf.

Un autre exemple...  
On peut modifier la valeur dans le **fichier /proc/sys/dev/cdrom/lock** en exécutant la **commande sysctl**.   
L'argument de la commande est le chemin d'accès au fichier que l’on modifie, en utilisa**nt le . entre le répertoire et le nom du fichie**r, par rapport au répertoire /proc/sys …   
**>>** **cat /proc/sys/dev/cdrom/lock**1   
**>> sudo sysctl dev.cdrom.lock=0   
dev.cdrom.lock = 0**   
**>>** **cat /proc/sys/dev/cdrom/lock**  
**0**

La commande sysctl précédente modifie uniquement le contenu actuel du fichier /proc/sys/dev/cdrom/lock.  
Si le système était redémarré, la **valeur de ce fichier serait 1 après le redémarrage** car il s'agissait de la valeur par défaut du système.

Pour en **faire un changement persistant** (en l’occurrence, identique après un redémarrage), on édite le fichier **/etc/sysctl.conf** et on ajoute un paramètre …   
**dev.cdrom.lock = 0**

**Remarque** …  
Sur les **anciennes distributions**, seul le **fichier /etc/sysctl.conf est utilisé** pour les paramètres du noyau.   
Sur les **distributions plus récentes**, il existe **quelques emplacements supplémentaires** où les paramètres du noyau peuvent être définis …   
**/usr/lib/sysctl.d/00-system.conf**

Les paramètres par défaut du système sont généralement placés (probablement ceux créés par le fournisseur de la distribution) dans le **répertoire /etc/sysctl.d**.

Ce répertoire peut contenir des fichiers de configuration supplémentaires, généralement sous le format de nom de nom **##.conf où ## représente un nombre compris entre 00 et 99**.

Le gros avantage de ce répertoire est désormais que les **éditeurs de logiciels peuvent ajuster les paramètres du** **noyau** en plaçant des fichiers dans ce répertoire lors de l'installation du logiciel (et en supprimant les fichiers lorsque le logiciel est désinstallé) plutôt que d'essayer de modifier directement le fichier /etc/sysctl.conf.

Le **numéro a pour but de créer un ordre**.   
Donc, **xyz04.conf serait utilisé avant abc05.conf**.

### Emplacements /proc/sys

Afin de s’y retrouver, voici la liste des emplacements /proc/sys ...

|  |  |
| --- | --- |
| Emplacement /proc/sys | Description |
| /proc/sys/dev/ | Ce répertoire contient les modifications des périphériques du système |
| /proc/sys/fs/ | Ce répertoire contient les modifications des paramètres du système de fichier  (informations de quota, de descripteur de fichier, d'inode et de dentry) |
| /proc/sys/kernel/ | Ce répertoire contient une variété de fichiers de configuration différents qui affectent directement le fonctionnement du noyau |
| /proc/sys/net/ | Ce répertoire contient les différentes configurations liées au réseau répertoires,  tels que Ethernet, IPv4, IPX, et IPv6 |
| /proc/sys/net/ipv4/ | Ce répertoire contient des paramètres réseau supplémentaires Un grand nombre de ces paramètres, utilisés en conjonction les uns avec les autres, sont utiles pour empêcher les attaques sur le système ou lors de l'utilisation du système comme routeur |
| /proc/sys/vm/ | Ce répertoire facilite la configuration du sous-système de mémoire virtuelle du noyau e noyau fait une utilisation intensive et intelligente de la mémoire virtuelle, communément appelée espace d'échange |

## Partitions de disque

La **séparation des fichiers du système d'exploitation des fichiers utilisateur** peut mener à un **système plus solide et sécurisé**.

Il peut être intéressant que les **systèmes de fichiers** suivants sont **montés sur des partitions distinctes** ...

* **/usr** ;
* **/home** ;
* **/var** et **/var/tmp** ;
* **/tmp**.

Il est préférable de **créer des partitions distinctes** pour les **répertoires racine** (root) des **serveurs Apache** et **FTP**.

Il est également intéressant de modifier le **fichier /etc/fstab** et de **s’assurer** **d'y ajouter les options de configuration suivantes** ...

* **noexec**  
  **Interdiction d'exécution de binaires** sur cette partition   
  (empêche l'exécution de binaires mais autorise les scripts) ;
* **nodev**  
  **Interdiction des caractères ou les périphériques spéciaux** sur cette partition   
  (empêche l'utilisation de fichiers de périphériques tels que zero, sda, ....) ;
* **nosuid**   
  **Interdiction des accès SUID/SGID** sur cette partition   
  (empêcher le bit setuid).

Voici un exemple d'entrée pour le fichier /etc/fstab afin de **limiter l'accès des utilisateurs** sur /dev/sda3   
(répertoire racine du serveur ftp) …  
**/dev/sda3 /ftpdata ext4 par defaults,nosuid,nodev,noexec 1 2**

### Point de montage systemd

On peut également créer un **point de montage systend**.

Voici un exemple de fichier /etc/systemd/system/ftpdata.mount dont le contenu est ce qui suit …  
**[Unit]  
Description=Montage du réoertoire racine (root) du service FTP**

**[Mount]  
What=/dev/sda3  
Where=/ftpdata  
Type=ext4  
Options=noatime,nosuid,nodev,noexec,mode=1777**

**[Install]  
WantedBy=multi-user.target**

On doit par la suite exécuter les commandes …   
**>> sudo systemctl start ftpdate.mount**  
pour démarrer le point de montage  
et  
**>> sudo systemctl enable ftpdate.mount**   
pour l'activer au démarrage.

**Remarques**...   
Il faudra ajouter une **section [Install] et un WantedBy=local-fs.target pour pouvoir l'activer avec succès**.  
**Ne pas oublier de supprimer la ligne correspondante du fichier /etc/fstab**, sinon le point de montage pourrait générer un conflit.   
**Après la création d’un fichier systemd**, il est d’usage de passer la commande suivante …  
**>> sudo systemctl daemon-reload**

## Quotas de disque

L’imposition de quotas de disque permet **d’éviter qu’un ou des utilisateurs monopolisent une bonne partie de l’espace disque**.  
Il est important de s’assurer que le **quota de disque est activé pour tous les utilisateurs**.

Pour mettre en œuvre des quotas de disque, il faut ...

* **Activer les quotas par système de fichiers** en modifiant le **fichier /etc/fstab** ;
* **Remonter le(s) système(s) de fichiers** ;
* **Créer les fichiers de base de données de quotas** et **générer la table d'utilisation du disque** ;
* **Attribuer des stratégies de quota**.

Voir le document complémentaire pour plus d’information.

## Désactivation du protocole IPv6

Internet Protocol version 6 (IPv6) fournit une nouvelle couche Internet de la suite de protocoles TCP/IP qui remplace Internet Protocol version 4 (IPv4) et offre de nombreux avantages.

**Si on n'utilise pas IPv6, il faut le désactiver**. Cela peut **augmenter la vitesse et la sécurité de la navigation**.

IPv6 est activé par défaut car presque toutes les distributions l'activent.

Pour **désactiver IPv6** …  
**>> sudo nano /etc/sysctl.conf**

Pour **désactiver IPv6 sur toutes les interfaces** à l'échelle du système …  
**net.ipv6.conf.all.disable\_ipv6 = 1**

On **décommente les deux lignes suivantes pour activer la protection contre l'usurpation** (filtre de chemin inverse).  
On active la vérification de l'adresse source dans toutes les interfaces pour éviter certaines attaques d'usurpation d'identité ...  
**net.ipv4.conf.default.rp\_filter=1  
net.ipv4.conf.all.rp\_filter=1**

On **n’accepte pas les redirections ICMP** (empêcher les attaques MITM) ...  
**net.ipv4.conf.all.accept\_redirects = 0  
net.ipv6.conf.all.accept\_redirects = 0**

On **n’envoie pas de redirections ICMP** (le serveur n’est pas un routeur) ...  
**net.ipv4.conf.all.send\_redirects = 0**

On **n’accepte pas les paquets de route source IP** (le serveur n’est pas un routeur) …  
**net.ipv4.conf.all.accept\_source\_route = 0  
net.ipv6.conf.all.accept\_source\_route = 0**

On **évite les échanges excessifs** …  
**vm.swappiness=0**

On **demande au système de prendre en considération les changements** …  
**>> sudo sysctl -p /etc/sysctl.conf**

On **poursuit la désactivation** …  
**>>** **sudo echo 'net.ipv6.conf.all.disable\_ipv6 = 1' > /etc/sysctl.d/90-disable-ipv6.conf  
>>** **sudo sysctl -p -f /etc/sysctl.d/90-disable-ipv6.conf**

Cette dernière étape s'applique uniquement **si on utilise SSH en mode démon** (sur un serveur) …  
**>> sudo nano /etc/ssh/sshd\_config**On **modifie la directive suivante** …  
**addressFamily inet**  
On **redémarre le service** ...  
**>> sudo systemctl restart ssh**

## Désactivation des binaires SUID et SGID indésirables

Tous les **fichiers étiquetés avec les bits SUID/SGID peuvent être mal utilisés** **lorsque l'exécutable SUID/SGID a un problème de sécurité ou un bogue**.   
Tout utilisateur local ou distant peut utiliser ce fichier.

>> ls -l /bin/mount   
-rwsr-xr-x 1 root root 44304 mar 7 2018 /bin/mount   
**>> ls -/usr/bin/passwd  
-rwsr-xr-x 1 root root 59680 mai 17 2017 /usr/bin/passwd**

Cela est une bonne idée d'**identifier tous ces fichiers**.   
On peut utiliser la **commande find** comme suit …  
**>> find <Répertoire> -type d -perm –4000  
>> find <Répertoire> -type d -perm –2000  
>> find <Répertoire> -type d -perm -1000  
>> find <Répertoire> \( -perm -4000 -o -perm -2000 \) -prin  
>> find <Répertoire> -path -prune -o -type f -perm +6000 -ls**

On doit **vérifier la pertinence de chaque fichier trouvé**.   
On peut consulter la page de manuel du fichier identifié pour plus de détails.

Pour plus d’information, voir le document …  
Autorisations de fichier spéciales

## Fichiers modifiables par tous les utilisateurs

N'importe quel utilisateur peut modifier un **fichier accessible en écriture pour tout le monde**, ce qui entraîne un **problème de sécurité**.   
Pour **trouver tous les fichiers d'ensembles de bits inscriptibles et collants** …  
**>> find <Répertoire> -type d \( -perm -0002 -a ! -perm -1000 \) -print**

On doit vérifier chaque fichier identifié et définir les autorisations d'utilisateur et de groupe appropriées ou, encore les supprimer.

## Identification des fichiers orphelins

Les **fichiers n'appartenant à aucun utilisateur ou groupe** peuvent **introduire un problème de sécurité**.   
On peur **rechercher les fichiers qui n'appartiennent pas à un utilisateur valide ou à un groupe valide** …   
**>> find <Répertoire> -xdev \ (-nouser -o -nogroup \) -print**

On doit vérifier chaque fichier identifié et éventuellement l'attribuer à un utilisateur et/ou un groupe approprié ou encore le supprimer.

## Utilisation d’un service d'authentification centralisé

**Sans système d'authentification centralisé**, les **données d'authentification des utilisateurs peuvent devenir incohérentes**. Cela peut éventuellement **entraîner des informations d'identification obsolètes** et **des comptes oubliés** qui auraient dû être supprimés.

Un service d'authentification centralisé permet de **maintenir un contrôle central sur les données de compte et d'authentification** Linux. Il est possible de **garder les données d'authentification synchronisées entre les serveurs**.

Il est préférable d’utiliser le **gestionnaire d’annuaire openLDAP** pour les clients et les serveurs au lieu de NIS pour l'authentification centralisée.

### Kerberos

Kerberos effectue l'authentification en tant que ser**vice d'authentification tiers de confiance en utilisant un secret cryptographique partagé**.

Les paquets circulant sur le réseau non sécurisé peuvent être lus, modifiés et insérés.

Kerberos s'appuie sur le chiffrement à clé symétrique et nécessite un centre de distribution de clés.   
On peut alors rendre la connexion à distance, la copie à distance, la copie sécurisée de fichiers inter-systèmes et d'autres **tâches à haut risque plus sûres et plus contrôlables à l'aide de Kerberos**.

Ainsi, lorsque les utilisateurs s'authentifient auprès des services réseau à l'aide de Kerberos, les **utilisateurs non autorisés tentant de collecter des mots de passe en surveillant le trafic réseau** sont efficacement contrecarrés.

## Journalisation et audit

Il est essentiel de **configurer la journalisation et l'audit afin de collecter toutes les tentatives de piratage et de craquage**.

Par défaut, **syslog ou journalctl** stocke les données dans le répertoire /var/log/.

Ceci est également utile pour **découvrir une mauvaise configuration d’un logiciel** qui peut exposer un hôte à diverses attaques.

Presque tous les fichiers journaux se retrouvent dans le **répertoire /var/log et ses sous-répertoires**.

**Remarque** …  
On doit être l'utilisateur **root pour accéder aux fichiers journaux**.

On peut utiliser les commandes suivantes pour **afficher les fichiers journaux qui sont au format texte**...

* commande **less** ;
* commande **more** ;
* commande **cat** ;
* commande **grep** ;
* commande **head** ;
* commande **tail** ;
* commande **zcat** (pour les fichiers compressés) ;
* commande **zgrep** (pour les fichiers compressés) ;
* commande **zmore** (pour les fichiers compressés) ;
* commande **dmesg** (pour les messages du noyau – au dmarrage) ;
* commande **journalctl** (systemd).

Pour afficher un fichier journal commun appelé /var/log/messages …  
**>> sudo less /var/log/messages  
>> sudo more -f /var/log/messages  
>> sudo cat /var/log/messages  
>> sudo tail -f /var/log/messages  
>> sudo grep -i error /var/log/messages**

Noms et utilisation courants des fichiers de journalisation

* **/var/log/messages**  
  Messages généraux et événements reliés au système
* **/var/log/auth.log**  
  Journaux d'authentification
* **/var/log/kern.log**  
  Journaux du noyau
* **/var/log/cron.log**  
  Journaux crond (tâche cron)
* **/var/log/maillog**  
  Journaux du serveur de messagerie
* **/var/log/httpd/** ou **/var/log/apache2**  
  Répertoire des journaux d'accès et d'erreurs d'Apache
* **/var/log/lighttpd/**  
  Répertoire des journaux d'accès et d'erreurs de Lighttpd
* **/var/log/nginx/**  
  Répertoire des journaux d'accès et d'erreurs de Nginx
* **/var/log/apt/**  
  Répertoire contenant l’historique des commandes et répertoire des journaux
* **/var/log/yum.log** ou /**var/log/dnf.log**  
  Fichier journal des commandes yum/dnf.
* **/var/log/boot.log**

Journal de démarrage du système

* **/var/log/mysqld.log**  
  Fichier journal du serveur de base de données MySQL
* **/var/log/secure** ou **/var/log/auth.log**  
  Journal d'authentification
* **/var/log/utmp** ou /**var/log/wtmp**  
  Fichier des enregistrements de connexion

### Impression des messages du tampon en anneau (*buffer ring*) du noyau Linux

La commande dmesg permet d’**examiner ou de contrôler le tampon en anneau du noyau**.

L'action par défaut est d'afficher tous les messages de la mémoire tampon en anneau du noyau …  
**>> sudo dmesg  
>> sudo dmesg | grep 'error'  
>> sudo dmesg | grep -i -E 'error|warn|failed'  
>> sudo dmesg | more**

### Commande journalctl (systemd)

systemd-journald est un **service système fourni avec systemd**.   
Il **collecte et emmagasine les données de journalisation**.

systemd-journald **crée et maintient des journaux structurés et indexés** basés sur les informations de journalisation reçues de **diverses sources** telles que les messages de journalisation du noyau Linux à l'aide de kmsg.

On utilise la **commande journalctl pour interroger le contenu du systemd-journald**.

Sans aucun argument, tous les journaux collectés sont affichés non filtrés …  
**>> sudo journalctl**

Affichage de tous les messages de démarrage   
**>> sudo journalctl --boot=1  
>> sudo journalctl -b 1**

Affichage des journaux du noyau du démarrage précédent …  
**>> sudo journalctl --kernel –boot=-1  
>> sudo journalctl -k -b -1**

Affichage d’un journal par unité ou service systemd  
**>> sudo ournalctl unit=apache2   
>> sudo journalctl unit=nginx   
>> sudo ournalctl -u apache2  
>> sudo journalctl -u nginx**

Affichage de journal en temps réel   
**>> sudo ournalctl --follow  
>> sudo journalctl -f  
>> sudo journalctl --follow --unit=nginx  
>> sudo journalctl -f -u nginx**

Le commutateur -u peut être utilisé plusieurs fois ...  
**>> sudo journalctl --unit=apache2.service --unit=php-cgi.service --unit=mysqld.service   
>> sudo journalctl -u apache.service -u php-cgi.service -u mysqld.service**

Affichage des 10 dernières entrées de journal :=…  
**>> sudo journalctl --lines=I0 –unit=nginx.service   
>> sudo journalctl -n 10 -u nginx.service**

Affichage en function du temps  
**>> sudo journalctl --since "30 min ago"  
>> sudo journalctl --since "1 hour ago"  
>> sudo journalctl --since "1 days ago"  
>> sudo journalctl --since "2020-06-06"  
>> sudo journalctl --since "2020-06-06 10:42:00"  
>> sudo journalctl --since "2020-06-04 10:42:00" --until "2020-06-07 10:42:00"**Les dated et heures sont au format AAAA-MM-JJ HH:MM:SS (YYYY-MM-DD HH:MM:SS)

Affichage des événements par ID utilisateur (UID) ou PID  
**>> sudo journalctl \_UID = 300  
>> sudo journalctl \_PID = 4242**

Affichage inversé pour que les entrées les plus récentes soient affichées en premier  
**>> sudo journalctl --reverse   
>> sudo journalctl –r  
>> sudo journalctl -r -u apache.service   
>> sudo journalctl --reverse –unit=sshd.service**

Affichage des messages du noyau Linux  
**>> sudo journalctl --dmesg  
>> sudo journalctl -k**

Filtrage des fichiers journaux (syntaxe comme grep)

Il est possible de filtrer la sortie vers les entrées où le champ MESSAGE = correspond à l'expression régulière spécifiée.   
**>> sudo journalctl --dmesg --grep=<Motif>   
>> sudo journalctl -k -g <Motif>  
>> sudo journalctl --unit=sshd.service --grep=<Motif>  
>> sudo journalctl -u sshd.service -g <Motif>  
>> sudo journalctl –unit=nginx.service --grep='error'  
>> sudo journalctl -u nginx.service -g 'error'  
>> sudo journalctl --dmesg –grep=failed  
>> sudo journalctl -k -g failed**

Si le **motif est entièrement en minuscules**, la **correspondance est insensible à la casse**.   
**Sinon, la correspondance est sensible à la casse**.   
Cela peut être remplacé par l'**option --case-sensitive**.

### Rotation des journaux

L’outil appelé **logrotate est conçu afin de faciliter l'administration des systèmes** qui génèrent un grand nombre de fichiers journaux.   
Il **permet la rotation**, **la compression**, **la suppression** et **l'envoi automatiques** des fichiers journaux.

Chaque **fichier journal** peut être géré **quotidiennement**, **hebdomadairement**, **mensuellement** ou lorsqu'il **devient trop volumineux**.

Avec logrotate, il est possible de **conserver les journaux plus longtemps**, et ce avec **moins d'espace disque**.

Le **fichier de configuration par défaut est /etc/logrotate.conf** …  
**# see "man logrotate" for details**

**# rotate log files weekly  
weekly**

**# keep 4 weeks worth of backlogs  
rotate 4**

**# create new (empty) log files after rotating old ones  
create**

**# use date as a suffix of the rotated file  
#dateext**

**# uncomment this if you want your log files compressed  
#compress**

**# packages drop log rotation information into this directory  
include /etc/logrotate.d**

**# system-specific logs may be also be configured here.**

où ...

* **weekly** (hebdomadaire)  
  Les fichiers journaux sont tournés si le jour de la semaine en cours est inférieur au jour de la dernière rotation ou si plus d'une semaine s'est écoulée depuis la dernière rotation ;
* **rotate 4** (rotation)  
  Les fichiers journaux subissent une rotation 4 fois avant d'être supprimés ou envoyés à l'adresse spécifiée dans une directive de messagerie.   
  Si cette valeur est égale à 0, les anciennes versions sont supprimées au lieu d'être tournées ;
* **compress** (compression)  
  Les anciennes versions des fichiers journaux sont compressées avec gzip afin d’économiser de l'espace disque ;
* **include**  
  Liaison vers les fichiers du répertoire donné en argument comme s'ils étaient inclus  
  Ces fichiers sont lus là où la directive d'inclusion apparaît.

Autres paramètres ...

* **missingok**  
  Si le fichier journal est manquant, on passe au suivant sans émettre de message d'erreur ;
* **notifempty**  
  Ne pas faire pivoter le journal s'il est vide ;

### Utilitaires Logwatch et Logcheck

Il peut être intéressant de **consulter les journaux à l'aide de la commande logwatch** (logcheck).   
Ces **utilitaires facilitent la lecture des journaux**.   
On obtient des **rapports détaillés sur les éléments inhabituels** dans syslog par courriels.

**Références** …  
**Logwatch**  
[**https://wiki.archlinux.org/title/Logwatch#:~:text=Logwatch%20is%20a%20powerful%20and,the%20command%20line%20or%20email**](https://wiki.archlinux.org/title/Logwatch#:~:text=Logwatch%20is%20a%20powerful%20and,the%20command%20line%20or%20email)**.**

**Logcheck**  
[**https://www.ictforce.be/2018/linux-security-logcheck/**](https://www.ictforce.be/2018/linux-security-logcheck/)

### Audition du système avec auditd

L'utilitaire auditd a comme objectif l’audition d’un système.   
Il est **responsable de l'écriture des enregistrements d'audit sur le disque**.

Au démarrage, les **règles dans le fichier /etc/audit.rules sont lues par le démon**.   
Il est possible d’apporter des modifications à ce fichier telles que l'emplacement du journal du fichier d'audit de configuration et d'autres options.

auditd procure des **informations concernant les éléments suivants** ...

* **Événements de démarrage et d'arrêt** **du système** ;
* **Date et heure d'un événement** ;
* **Utilisateur qui est responsable d'un événement** ;
* **Type d'événement**   
  (modification, accès, suppression, écriture, mise à jour d’un objet et commandes) ;
* **Succès ou échec d'un événement** ;
* **Événements qui modifient la date et l'heure**.
* **Utilisateur(s) ayant apporté des modifications à un objet** (fichier, répertoire, …) ;
* **Utilisateur(s) ayant apporté des modifications aux paramètres réseau du système** ;

Événements qui modifient les informations des utilisateurs/groupes.

Pour plus d’information, voir le document …  
auditd

# Sécuriser le service openSSH

Le protocole **SSH est recommandé pour la connexion à distance** et le **transfert de fichiers à distance**.   
Cependant, **SSH est ouvert à de nombreuses attaques**.

Pour plus d’information, voir le document …  
Bonnes pratiques de configuration SSH

# Système de détection/prévention d'intrusion

Un système de détection/prévention d'intrusion réseau (NIDS ou NIPS) est un **système qui tente de détecter les activités malveillantes** telles que …

* les **attaques par déni de service** ;
* les **analyses de ports**   
  ou même
* les **tentatives de piratage des hôtes** en surveillant le trafic réseau.

Il est **recommandé de déployer tout logiciel de vérification d'intégrité** **avant que le système ne soit mis en ligne** dans un environnement de production.

Si possible, installez le **logiciel AIDE avant que le système ne soit connecté à un réseau**.   
AIDE est un système de détection d'intrusion basé sur l'hôte (HIDS) qui peut surveiller et analyser les composants internes d'un système informatique.

Il est aussi recommandé d'installer et d'utiliser également le **logiciel de détection de rootkit rkhunter**.

Avec les informations sur les fichiers, AIDE vérifie les attributs des fichiers tels que …

* le **type de fichier** ;
* les **autorisations** ;
* le **GID** ;
* l'**UID** ;
* la **taille** ;
* le **nom du lien** ;
* le **nombre de blocs** ;
* le **nombre de liens** ;
* les **attributs mtime**, **ctime** et **atime**   
  et
* les **attributs générés** par **XAttrs**, **SELinux**, **Posix** **ACL** et **Extended**.

# Désactivation des périphériques USB/Firewire/Thunderbolt

Il est possible de **désactiver la clé USB ou les disques durs**, que les utilisateurs peuvent **utiliser avec un accès physique** à un système afin de **copier rapidement des données sensibles** à partir de celui-ci.

Le lecteur de stockage USB détecte automatiquement les clés USB ou les disques durs.   
On peut rapidement **forcer et désactiver les périphériques de stockage USB** sous n'importe quelle distribution Linux.

L’**utilitaire** **modprobe** est utilisé pour le **chargement automatique des modules du noyau**.  
Il peut être **configuré afin de ne pas charger le pilote de stockage USB** à la demande.  
Cela **empêchera le programme modprobe de charger le module de stockage USB**, mais **n'empêchera pas root** (ou un autre programme privilégié) **d'utiliser les utilitaires** **insmod/modprobe** pour charger le module manuellement.

Des **clés USB contenant des logiciels malveillants nuisibles** peuvent être utilisées pour voler les données. Il n'est pas rare que des clés USB soient utilisées pour **transporter et transmettre des logiciels malveillants** et des **virus** **destructeurs aux ordinateurs**.

## Pilote de stockage USB

Le **fichier usb-storage.ko contient le pilote de stockage de masse USB** pour un système Linux …  
**>> ls -l /lib/modules/$(uname -r)/kernel/drivers/usb/storage/usb-storage.ko**

Il est possible de **désactiver ou de supprimer le pilote usb-storage.ko afin de restreindre l'utilisation de périphériques USB** sous Linux tels que ...

* **clavier** USB ;
* **souris** USB ;
* **clé** USB ;
* **disque d**ur USB ;
* tout **autre stockage de bloc** USB.

On peut **supprimer le pilote de stockage USB sans redémarrer le système** …  
**>> sudo modprobe -r usb-storage  
>> mv -v /lib/modules/$(uname -r)/kernel/drivers/usb/storage/usb-storage.ko /root/  
>> sudo lsmod | grep -i usb-storage**

## Liste noire

On édite le **fichier /etc/modprobe.d/blacklist.conf** …  
**>> sudo nano /etc/modprobe.d/blacklist.conf**

On modifie ou on ajoute …  
**blacklist usb-storage**

On enregistre et on ferme le fichier.

## Option BIOS

On peut également désactiver l'USB à partir de l'**option de configuration du BIOS système**.   
On doit toutefois **s’assurer que le BIOS est protégé par mot de passe**.   
Il s'agit d'une **option recommandée afin que personne ne puisse le démarrer à partir de l'USB**.

## Chiffrement **du** disque dur

Linux prend en charge les différentes techniques cryptographiques pour protéger un disque dur, un répertoire et une partition.

## Option du GRUB

On peut se débarrasser de tous les périphériques USB en désa**ctivant la prise en charge du noyau pour USB à partir du GRUB**.

On ouvre le **fichier grub.cfg et on ajoute nousb à la ligne débutant par linux** …  
**kernel /vmlinuz-2.6.18-128.1.1.el5 ro root = LABEL = / console = tty0 console = ttyS1,19200n8 nousb**

On doit s’assurer de **supprimer toute autre référence au stockage USB** dans les fichiers de configuration grub ou grub2. On enregistre et on ferme le fichier.

Une fois cela fait, il suffit de redémarrer le système.

# Fail2ban comme IDS

Fail2ban analyse les fichiers journaux à la **recherche d'un trop grand nombre de tentatives de connexion infructueuses** et **bloque l'adresse IP** qui affiche des signes malveillants.

**Exposer un serveur sur Internet comporte des risques**.  
Un des plus importants est les nombreuses attaques par effraction et par force brute.

L’**utilitaire** **denyHosts** est un **outil de sécurité de prévention des intrusions basé sur les journaux pour les serveurs SSH**. Il est conçu pour empêcher les attaques par force brute sur les serveurs SSH en surveillant les tentatives de connexion non valides dans le journal d'authentification.   
Toutefois, cet **outil ne fait plus l’objet d’un développement actif**.

## Installation de fail2ban

Pour installer fail2ban…  
**>> sudo apt install fail2ban   
>> sudo yum|dnf install fail2ban   
>> sudo zypper install fail2ban**

On modifie le fichier de configuration selon ses besoins …  
**>> sudo nano /etc/fail2ban/jail.conf**

On doit redémarrer le service à la suite de la modification du fichier de configuration …  
**>> sudo sudo systemctl restart/reload fail2ban.service**

Pour plus d’information, voir le document …  
fail2ban

Comme autre IDS, il est aussi possible d’utiliser les **utilitaires AIDE** (*Advanced Intrusion Detection Environment*) qui **surveille l’utilisation frauduleuse de fichiers et répertoires**.  
**PSAD** (Port Scan Attack Detector) permet de **détecter et bloquer les attaques par analyse de port en temps réel**.

# Protection des fichiers, des répertoires et des disques

Linux propose de **nombreuses options contre les accès non autorisés aux données**.   
Les **autorisations de fichiers** (dont MAC) **empêchent les accès non autorisés** d'accéder aux données.

Cependant, les autorisations définies par Linux **ne sont pas pertinentes si un attaquant possède un accès physique à un** **système** et peut simplement **déplacer le disque dur de l'ordinateur** **vers un autre système** afin de copier et analyser les données sensibles.

On peut **facilement protéger les fichiers et partitions sous Linux** en utilisant les **outils suivants** …

* **Chiffrement et déchiffrement des fichiers** avec un mot de passe à l’aide de **gpg** ;
* Un **mot de passe protégeant les fichiers avec mcrypt** ou **openssl** ;
* Le **chiffrement complet du disque** est indispensable pour sécuriser les données et est pris en charge par la plupart des distributions Linux.  
  On peut chiffrer un **disque dur à l'aide de LUKS** sous Linux ;
* On s’assure que la **partition (ou fichier) swap est également chiffré** ;
* On doit **exiger un mot de passe pour modifier le chargeur de démarrage**.

# Sauvegardes

On ne soulignera jamais assez à quel point il est **important de faire une sauvegarde d'un système Linux**.

Une **sauvegarde hors site appropriée permet de récupérer à partir d'un serveur endommagé**, suite à une intrusion.

Les **programmes de sauvegarde Linux traditionnels sont le vidage et la restauration** sont également recommandés.

# Autres recommandations