

# *Guide hardening LINUX*

*En date du 25 mars 2021*





### Rédaction

Date	Prénom Nom	Fonction	Action	Statut
	Jérémie <b>RODRIGUEZ</b>	Etudiant Ynov	Rédaction	OK
	Thibaut <b>SANJUAN</b>	Etudiant Ynov	Rédaction	OK

### Suivi de version

Version	Auteur	Dates	Commentaires
1.0	Jérémie <b>RODRIGUEZ</b> Thibaut <b>SANJUAN</b>	25/03/2021	



## TABLE DES MATIERES

<b>TABLE DES MATIERES</b>	<b>2</b>
<b>1. INFORMATIONS</b>	<b>4</b>
A. DEFINITION DU GUIDE	4
B. CIBLE ET NIVEAU DE DURCISSEMENT	4
<b>2. PRECONISATIONS D'USAGE</b>	<b>5</b>
A. PLUSIEURS COMPTES : PRIVILEGES RESTREINTS – PRIVILEGE ELEVES	5
B. CHANGEMENT DES MOTS DE PASSE PAR DEFAUT :	5
C. MOT DE PASSE ROBUSTE :	5
D. POLITIQUE DE CHANGEMENT DE MOT DE PASSE :	5
E. GESTIONNAIRE DE MOT DE PASSE :	5
F. ENCADRER SA NAVIGATION SUR INTERNET :	6
G. LIMITER L'EXPOSITION D'INFORMATIONS SUR LES RESEAUX SOCIAUX :	6
H. ENCADRER SES ECHANGES PAR EMAILS :	6
I. VERIFIER REGULIEREMENT LES ADRESSES MAILS ET MOTS DE PASSE UTILISES	6
J. NE PAS ECRIRE SES MOT DE PASSES DE FAÇON VISIBLE PHYSIQUEMENT ET NUMERIQUEMENT	7
K. DISPOSER D'UN ANTI-VIRUS A JOUR AVEC UN PARE FEU ACTIF	7
L. NE PAS EXPOSER DE SERVICE SUR INTERNET SANS SECURITE	7
M. OUTILS ET LOGICIELS PRECONISES POUR REDUIRE L'EXPOSITION A LA FUITE D'INFORMATIONS	7
<b>3. GUIDE DE HARDENING ET MODE OPERATOIRE</b>	<b>8</b>
A. ARCHITECTURE SERVEUR - DESKTOP	8
B. SECURITE PHYSIQUE SERVEUR - DESKTOP	8
C. SECURITE BIOS/UEFI SERVEUR - DESKTOP	8
D. PARTITIONNEMENT SERVEUR - DESKTOP	9
E. CHIFFREMENT DES DISQUES SERVEUR - DESKTOP	10
F. UTILISATION DE SUDO SERVEUR - DESKTOP	10
G. UTILISATION DE VERSIONS SECURISEES DE SERVICES SERVEUR - DESKTOP	11
H. APPLIQUER LES MISES A JOUR SERVEUR - DESKTOP	11
I. UN SERVICE RESEAU PAR INSTANCE- PAS DE SERVICE NON DESIRE SERVEUR	11
J. DESACTIVATION DES SERVICES NON SOUHAITES SERVEUR - DESKTOP	12
K. CONFIGURER SELINUX OU APPARMOR SERVEUR - DESKTOP	12
L. INSTALLER SOPHOS ANTIVIRUS – HIDS POUR LINUX SERVEUR - DESKTOP	13
M. SECURISER SSH SERVEUR - DESKTOP	13
N. CONFIGURER IPTABLES SERVEUR	14
O. CONFIGURER FAIL2BAN OU CROWDSEC SERVEUR – DESKTOP	15
P. CHANGER MOT DE PASSE AU PREMIER LOGIN ET IMPLEMENTER UNE DATE D'EXPIRATION SERVEUR – DESKTOP	15
Q. JOURNALISATION DES EVENEMENTS SERVEUR – DESKTOP	16
R. DESACTIVER IPV6 SI NON UTILISE SERVEUR – DESKTOP	16
S. TACHES PLANIFIEES – CRON SERVEUR – DESKTOP	17
T. CONTROLER LES PORTS EN ECOUTE SUR LE RESEAU SERVEUR – DESKTOP	17
U. DROITS SUR LES FICHIERS ET EXECUTABLES / FICHIERS SENSIBLES SERVEUR – DESKTOP	18
V. CONFIGURER DES SAUVEGARDES SERVEUR – DESKTOP	20
W. ENUMERATION GLOBALE VIA SCRIPT SERVEUR – DESKTOP	20



X. PARTAGES ET PROTOCOLE SAMBA (SMB) SERVEUR – DESKTOP	20
Y. CHERCHER ROOTKITS – HARDENING TARDIF SERVEUR – DESKTOP	21
Z. AUDIT AUTOMATISEE DES VULNERABILITES SERVEUR – DESKTOP	21
AA. SOURCES	<b>ERREUR ! SIGNET NON DEFINI.</b>



## 1. .... INFORMATIONS

### A. DEFINITION DU GUIDE

Ce guide a pour but de sensibiliser aux bonnes pratiques liées à l'utilisation du système d'exploitation Linux ainsi que de durcir la configuration des machines afin d'accroître leur sécurité et leur résilience face aux menaces potentielles dans un système d'information.

### B. CIBLE ET NIVEAU DE DURCISSEMENT

OS LINUX : Debian, CentOS, Redhat, Ubuntu Server pour les versions disposant de support.





⚠ Dans le cas de l'existence d'un OS End of life la machine sera placée dans une DMZ (zone démilitarisée, isolée dans le réseau) et c'est cette zone qui sera sécurisée à défaut de pouvoir sécuriser ou durcir le système d'exploitation.

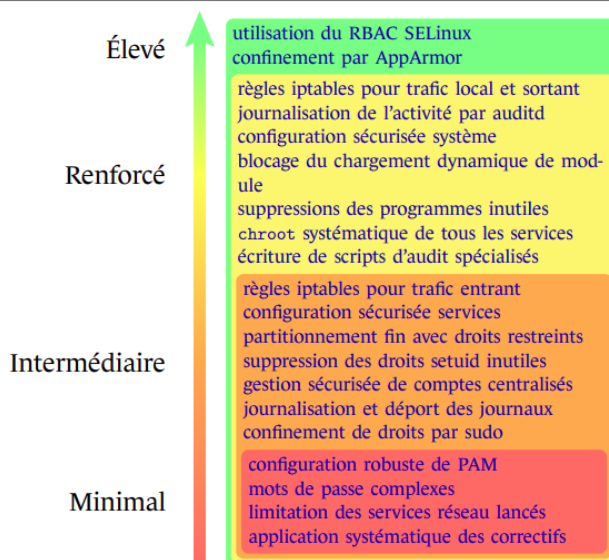
Basé sur le guide de configuration de l'ANSSI on peut visualiser plusieurs niveaux de sécurités.

Ce guide se base sur un niveau de sécurité renforcé à élevé.

[https://www.ssi.gouv.fr/uploads/2016/01/linux\\_configuration-fr-v1.2.pdf](https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf)

Ce guide est applicable aussi bien aux versions serveurs que desktop mais cible en priorité les serveurs Linux de production.

Niveau	Description
	Recommandation de niveau <b>minimal</b> . À mettre en œuvre systématiquement sur tout système.
	Recommandation à appliquer dès le niveau <b>intermédiaire</b> . Correspond généralement à des services protégés par plusieurs couches de sécurité de niveau supérieur.
	Recommandation s'appliquant dès le niveau <b>renforcé</b> . Généralement pour des systèmes exposés à des flux non authentifiés ou de sources nombreuses.
	Recommandation valide au niveau <b>élevé</b> . Correspond à des systèmes hébergeant des données sensibles accessibles depuis des réseaux non authentifiés ou peu contrôlés.





## 2. .... PRECONISATIONS D'USAGE

### A. *PLUSIEURS COMPTES : PRIVILEGES RESTREINTS – PRIVILEGE ELEVES*

L'utilisation d'un compte à privilège élevé doit être utilisée uniquement pour les actions d'administration.

L'utilisation courante de la machine doit être faite avec un compte à privilèges restreints. Notamment la navigation sur internet.

Les mots de passe de ces deux comptes doivent impérativement être différents.

### B. *CHANGEMENT DES MOTS DE PASSE PAR DEFAUT :*

Les mots de passe par défaut doivent systématiquement être changés au plus tôt.

### C. *MOT DE PASSE ROBUSTE :*

Un mot de passe robuste est préconisé pour les comptes.

Il est recommandé d'utiliser au moins 12 caractères alphanumériques avec majuscules et minuscules ainsi qu'au moins un caractère spécial en excluant des mots du dictionnaire ou des éléments liés à notre environnement ( nom d'entreprise, prénom) ou de contexte ( années, mois en cours...)

L'ANSSI propose un guide à ce sujet.

<https://www.ssi.gouv.fr/guide/mot-de-passe/>

Ainsi qu'un outil pour calculer la force des mots de passe

<https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/>

### D. *POLITIQUE DE CHANGEMENT DE MOT DE PASSE :*

Il est important de changer ses mots de passe, tous les 2 mois par exemple.

Cette politique est d'autant plus importante pour les comptes à privilèges élevés de type administrateur par exemple.

### E. *GESTIONNAIRE DE MOT DE PASSE :*



L'utilisation d'un coffre-fort pour gérer ses mots de passe est préconisée, cela permet d'utiliser des mots de passe robustes et éviter de stocker ses mots de passe sur la machine en clair par exemple dans le navigateur.

L'ANSSI recommande KEEPASS mais d'autres alternatives existent comme Bitwarden.

#### **F. ENCADRER SA NAVIGATION SUR INTERNET :**

La navigation sur internet doit être encadrée et maîtrisée. La navigation sur des sites douteux doit être proscrite et aucune information ne doit être échangée sur un site n'étant pas sécurisé. (adresse en http et non https)

Un lien sécurisé est matérialisé par un petit cadenas dans la barre de navigation au début de l'URL.

Aucun logiciel ou autre exécutable ne doit être téléchargé et exécuté s'il provient d'une source douteuse.

Utiliser un navigateur plus sécurisé comme Brave ou installer des extensions pour limiter les interactions du navigateur peut être une option. Extensions comme AD Block, Ghostery ect...

#### **G. LIMITER L'EXPOSITION D'INFORMATIONS SUR LES RESEAUX SOCIAUX :**

L'exposition d'informations sur les réseaux sociaux dans le cadre personnel ou professionnel est à encadrer et à contrôler.

Toute information divulguée peut permettre à une personne mal intentionnée de profiter de celle-ci pour une action malveillante.

#### **H. ENCADRER SES ECHANGES PAR EMAILS :**

Il est important de faire preuve de vigilance en manipulant ses courriers électroniques, surtout quand ils comportent des liens ou des pièces-jointes.

Il faut s'assurer de bien vérifier l'expéditeur réel du message et en cas de doute, n'effectuer aucune action.

Toute notion d'urgence dans un mail qui incite à action impliquant de cliquer sur un lien, de télécharger une pièce jointe ou d'appeler un numéro de téléphone pointe souvent un mail frauduleux.

#### **I. VERIFIER REGULIEREMENT LES ADRESSES MAILS ET MOTS DE PASSE UTILISES**



Des fuites de données ont lieu régulièrement suite à des compromissions de système d'information ou des erreurs de configurations de tiers détenteurs de données.

Les liens suivants permettent de vérifier si nos données ont été dérobées et s'il est nécessaire de changer ses mots de passe.

Adresse email :

<https://cybernews.com/personal-data-leak-check/>

<https://haveibeenpwned.com/>

Mot de passe :

<https://haveibeenpwned.com/Passwords>

**J. NE PAS ECRIRE SES MOT DE PASSES DE FAÇON VISIBLE PHYSIQUEMENT ET NUMERIQUEMENT**

Il est à proscrire d'écrire ses mots de passe sur papier ou post-it, ou encore sur des fichiers en clair sur son ordinateur comme un fichier texte.

L'utilisation d'un gestionnaire de mot de passe à la place est préconisée.

**K. DISPOSER D'UN ANTI-VIRUS A JOUR AVEC UN PARE FEU ACTIF**

Il est important de disposer d'un antivirus y compris sous une machine Linux.

Les antivirus modernes peuvent intégrer des fonctions avancées.

Il est possible de compléter cette protection avec un EDR ( Endpoint Detection and Response ) et un HIDS (host-base intrusion Detection Sytem)

Le guide aborde la solution choisie et le mode opératoire de sa mise en œuvre.

**L. NE PAS EXPOSER DE SERVICE SUR INTERNET SANS SECURITE**

Aucun service ne doit être exposé sur internet s'il ne dispose pas d'une sécurité adéquate et testée.

Certains services comme le protocole de bureau distant de Windows (RDP) ne doivent en aucun cas être exposés sur internet.

**M. OUTILS ET LOGICIELS PRECONISES POUR REDUIRE L'EXPOSITION A LA FUITE D'INFORMATIONS**





Le site [privacytools](https://www.privacytools.io/) propose différents logiciels et outils adaptés aux préconisations et aux bonnes pratiques mentionnées ci-dessus permettant de réduire son exposition et de se prémunir de certaines menaces.

<https://www.privacytools.io/>

### 3. .... GUIDE DE HARDENING ET MODE OPERATOIRE

#### A. ARCHITECTURE **SERVEUR** - **DESKTOP**

##### Architecture 64 bits :

Différentes architectures existent, dans le cadre de la production préférez l'installation d'un OS avec une architecture 64 bits

#### B. SECURITE PHYSIQUE **SERVEUR** - **DESKTOP**

##### Accès physique

L'accès physique à toute machine doit être restreint et encadré.  
Pour les serveurs de production, ils doivent être isolés dans un local dédié avec contrôle d'accès.

##### Désactiver ports USB (optionnel)

Editer le fichier blacklist.conf

```
#nano /etc/modprobe.d/blacklist.conf
```

Ajouter la ligne

```
blacklist usb_storage
```

Editer le fichier rc.local

```
#nano /etc/rc.local
```

Ajouter les lignes

```
modprobe -r usb_storage  
exit 0
```

#### C. SECURITE BIOS/UEFI **SERVEUR** - **DESKTOP**

##### Mot de passe



Le BIOS / UEFI de la machine doit être protégé par mot de passe.

Le mode opératoire pour y accéder dépendra de la machine physique. Souvent il s'agit d'une touche ou une combinaison de touches clavier à appuyer lors du démarrage.

### Ordre de démarrage :

L'ordre des périphériques pour le démarrage du BOOT ne doit pas permettre de démarrer depuis un périphérique externe (USB, CD, DVD..)

### Mise à jour du BIOS :

Il est possible de mettre à jour le BIOS des machines.

Il faut suivre la procédure préconisée par le constructeur du matériel.

## D. PARTITIONNEMENT **SERVEUR** - **DESKTOP**

Le partitionnement permet de protéger et d'isoler les composants du système de fichiers. Dans le cadre de l'utilisation intensive de certains points de montage, il est recommandé de les placer dans une partition voire un disque isolé.

Point de montage	Options	Description
/	<sans option>	Partition racine, contient le reste de l'arborescence
/boot	nosuid,nodev,noexec (noauto optionnel)	Contient le noyau et le chargeur de démarrage. Pas d'accès nécessaire une fois le boot terminé (sauf mise à jour)
/opt	nosuid,nodev (ro optionnel)	Packages additionnels au système. Montage en lecture seule si non utilisé
/tmp	nosuid,nodev,noexec	Fichiers temporaires. Ne doit contenir que des éléments non exécutables. Nettoyé après redémarrage ou préférentiellement de type <i>tmpfs</i>
/srv	nosuid,nodev (noexec,ro optionnels)	Contient des fichiers servis par un service type web, ftp, etc.
/home	nosuid,nodev,noexec	Contient les <i>HOME</i> utilisateurs. Montage en lecture seule si non utilisé
/proc	hidepid=2	Contient des informations sur les processus et le système
/usr	nodev	Contient la majorité des utilitaires et fichiers système
/var	nosuid,nodev,noexec	Partition contenant des fichiers variables pendant la vie du système (mails, fichiers PID, bases de données d'un service)
/var/log	nosuid,nodev,noexec	Contient les logs du système
/var/tmp	nosuid,nodev,noexec	Fichiers temporaires conservés après extinction

Le partitionnement est possible dès l'installation sur la majeure partie des distributions Linux.

Deux guides expliquent le partitionnement :

[https://doc.ubuntu-fr.org/tutoriel/partitionner\\_manuellement\\_avec\\_installateur\\_ubuntu](https://doc.ubuntu-fr.org/tutoriel/partitionner_manuellement_avec_installateur_ubuntu)



<https://lecrabeinfo.net/redimensionner-agrandir-reduire-une-partition-sur-linux.html>

### Sécuriser la partition du BOOT

La partition du boot doit être sécurisée car elle est reliée au kernel Linux.

Modifiez le fichier **/etc/fstab** en ajoutant

```
LABEL=/boot      /boot      ext2(ou autre format) defaults,ro      1 2
```

## E. CHIFFREMENT DES DISQUES **SERVEUR - DESKTOP**

Le chiffrement des disques permet d'améliorer la sécurité en réduisant les capacités d'accès aux données lorsque la machine est éteinte, en cas de perte ou encore de vol d'une machine.

### Chiffrement à l'installation :

Il est possible de chiffrer le ou les disques dès l'installation comme préciser dans la documentation ci-dessous pour ubuntu.

[https://doc.ubuntu-fr.org/tutoriel/chiffrer\\_son\\_disque](https://doc.ubuntu-fr.org/tutoriel/chiffrer_son_disque)

### Chiffrement après installation :

Il est aussi possible de chiffrer le disque après installation ou lors de l'ajout d'un disque.

<https://docs.oracle.com/en/database/other-databases/nosql-database/20.3/security/disk-encryption-linux-environment.html>

## F. UTILISATION DE SUDO **SERVEUR - DESKTOP**

L'utilisation de sudo à la place du compte root est à privilégier

Souvent installé par défaut sur les dernières versions de Linux il peut cependant être absent de certaines versions anciennes ou certaines versions sans « sudoers ».

Un guide détaille sont installation et son utilisation

<https://www.vultr.com/docs/how-to-use-sudo-on-debian-centos-and-freebsd>

- ⚠ Seuls les utilisateurs choisis doivent pouvoir accéder au groupe sudoers et effectuer des sudo.
- ⚠ NOPASSWD ne doit être utilisé pour sudo, ce qui équivaut à pouvoir passer une commande sudo sans taper de mot de passe.

Il est recommandé pour le fichier **/etc/sudoers** d'appliquer cette configuration :



*Defaults noexec,requiretty,use\_pty,umask=0027  
Defaults ignore\_dot,env\_reset,passwd\_timeout=1*

## G. UTILISATION DE VERSIONS SECURISEES DE SERVICES SERVEUR - DESKTOP

Les services de type FTP, Telnet, Rlogin, Rsh service doivent être évités au maximum au profit des services sécurisés comme :

SFTP (secure FTP) or FTPS (FTP over SSL) pour FTP  
SSH à la place de telnet

Pour supprimer les services non sécurisés sur Centos – Redhat :

```
#yum erase xinetd ypserv tftp-server telnet-server rsh-server
```

Pour supprimer les services non sécurisés sur Debian - Ubuntu

```
$ sudo apt-get --purge remove xinetd nis yp-tools tftpd atftpd tftpd-hpa  
telnetd rsh-server rsh-redone-server
```

## H. APPLIQUER LES MISES A JOUR SERVEUR - DESKTOP

Le système doit être mis à jour régulièrement pour appliquer les correctifs de sécurité au niveau du kernel linux ou des applicatifs et des services :

Pour Centos RedHat

```
#yum update
```

Pour Debian – Ubuntu :

```
$ sudo apt-get update && apt-get upgrade
```

## I. UN SERVICE RESEAU PAR INSTANCE- PAS DE SERVICE NON DESIRE SERVEUR

### Un service par instance

Pour des raisons de sécurité, il est recommandé de n'installer qu'un seul service réseau par instance.

Une instance peut être une machine virtuelle ou une machine dédiée le cas échéant :

Par exemple, on n'installera pas sur une même instance :

- Serveur WEB sur une instance
- Base de données sur une autre instance
- Serveur mail



- DNS

Dans le cas où plusieurs services non recommandés à la cohabitation seraient détectés, remontez l'information à votre responsable.

### J. DESACTIVATION DES SERVICES NON SOUHAITES **SERVEUR - DESKTOP**

Il est recommandé de désactiver les services non désirés sous Linux. Cela évitera potentiellement l'ouverture de ports inutiles ou encore l'exploitation de ces services

Gestion des services sous Ubuntu, Debian

<https://gastack.fr/ubuntu/19320/how-to-enable-or-disable-services>

Gestion des services sous RedHat, Centos

[https://access.redhat.com/documentation/fr-fr/red\\_hat\\_enterprise\\_linux/7/html/system\\_administrators\\_guide/sect-managing\\_services\\_with\\_systemd-services](https://access.redhat.com/documentation/fr-fr/red_hat_enterprise_linux/7/html/system_administrators_guide/sect-managing_services_with_systemd-services)

### K. CONFIGURER SELINUX OU APPARMOR **SERVEUR - DESKTOP**

SELinux et AppArmor sont deux extensions de sécurité dédiées à Linux. Activées par défaut sur les dernières versions, il est préconisé de les laisser active et d'en vérifier le fonctionnement.

#### SELinux

SELinux est activé par défaut sur les dernières versions de CentOS et RedHat.

SELinux renforce la sécurité et doit être activé.

Commande :

```
# getenforce
```

```
# sestatus
```

Lien pour vérifier le status de SELinux

<https://www.thegeekdiary.com/how-to-check-whether-selinux-is-enabled-or-disabled/>

Si SELinux n'est pas installé :

<https://www.digitalocean.com/community/tutorials/an-introduction-to-selinux-on-centos-7-part-1-basic-concepts>



## AppArmor

AppArmor est activé par défaut sur les dernière versions de Debian et Ubuntu.

AppArmor renforce la sécurité et doit être activé.

Commande :

```
aa-status
```

Lien pour vérifier le status de AppArmor

<https://www.unixtutorial.org/how-to-check-apparmor-status/>

Si AppArmor n'est pas installé :

<https://guide.ubuntu-fr.org/server/apparmor.html>

Explications de SELinux et AppArmor

<https://www.cyberciti.biz/tips/selinux-vs-apparmor-vs-grsecurity.html>

## L. INSTALLER SOPHOS ANTIVIRUS – HIDS POUR LINUX **SERVEUR - DESKTOP**

La politique de l'entreprise impose d'installer Sophos Intercept X (avec anti-virus) sur toutes les machines Linux.

La version de Sophos central intercept X est à télécharger depuis la console Sophos Central de l'entreprise.

Documentation officielle :

<https://www.sophos.com/fr-fr/support/documentation/sophos-anti-virus-for-linux.aspx>

Tutorial vidéo :

[https://www.youtube.com/watch?v=drFyRSmGOT8&ab\\_channel=SophosSupport](https://www.youtube.com/watch?v=drFyRSmGOT8&ab_channel=SophosSupport)

Tutorial détaillé ( à appliquer avec la version de Sophos téléchargée depuis Sophos Central):

<https://www.bleepingcomputer.com/forums/t/578679/sophos-antivirus-for-linux/>

## M. SECURISER SSH **SERVEUR - DESKTOP**

Pour sécuriser le SSH plusieurs actions sont à mener, un guide apportera le détail des modifications à la fin de l'énumération de celles-ci.



### **Optionnel : Changer le port SSH (défaut port 22)**

Changer le port SSH par défaut peut éviter les attaques automatiques mais ne sera pas efficace sur des attaques modernes.

### **Désactiver SSH pour ROOT :**

Il ne sera pas possible de se connecter en SSH avec le compte ROOT

### **Préconisé si possible : Désactiver SSH password login au profit d'une clé SSH**

Guide pour les actions ci-dessus :

<https://korben.info/tuto-ssh-securiser.html>

### **Pour desktop : Désactiver SSH si non nécessaire.**

Mode opératoire : Stopper le service SSH en se référant à la gestion des services du point « I » sur la désactivation des services

### **Optionnel : Message du jour ou MOTD**

Il faut modifier le fichier /etc/ssh/sshd\_config comme suit:

```
PrintMotd yes  
PrintLastLog yes
```

PrintMotd défini sur yes permettra d'afficher la bannière après connexion au serveur ssh tandis que PrintLastLog permet d'afficher dans la bannière la dernière connexion réussie.

L'autre élément intéressant serait d'afficher le nombre de tentatives infructueuses de connexions dans le MOTD.

Cela vient par défaut sur les serveurs CentOS mais pas sur debian, la commande ci-après nous révèle l'information voulue:

```
echo -ne "Total des tentatives échouées: $(grep 'Failed password' /var/log/auth.log* | wc -l)  
failed attempts"
```

source : <https://www.kali-linux.fr/astuces/comment-securiser-son-serveur-ssh>

## **N. CONFIGURER IPTABLES SERVEUR**

Iptables fait office de parefeu. Sur les serveurs accessibles depuis internet, il faut s'assurer que le service SSH soit restreints aux seules IP publiques de l'entreprise.



La commande suivante n'autorise le SSH que depuis l'IP publique de l'entreprise et drop le reste des connexions SSH :

```
iptables --append INPUT --protocol all --dst <IP publique> --dport 22 --jump DROP
```

### O. CONFIGURER FAIL2BAN OU CROWDSEC **SERVEUR – DESKTOP**

Selon la machine votre responsable vous indiquera la version à installer et la configuration spécifique le cas échéant :

#### **Fail2Ban :**

Fail2ban permet de sécuriser d'avantage les protocoles comme SSH en filtrant les IP qui tenteraient du bruteforce.

Guide fail2ban :

<https://www.linuxtricks.fr/wiki/fail2ban-bannir-automatiquement-les-intrus>

#### **CrowdSec :**

CrowdSec est le successeur de fail2ban est permet en plus de détecter les actions potentiellement malveillantes il permet de bénéficier de retour de la communauté avec de la threat intelligence pour bannir les IP ayant été détectées comme exerçant des actions malveillantes.

Guide crowdsec :

<https://crowdsec.net/2021/01/18/get-started-with-crowdsec-v1/>

### P. CHANGER MOT DE PASSE AU PREMIER LOGIN ET IMPLEMENTER UNE DATE D'EXPIRATION **SERVEUR – DESKTOP**

Il est recommandé d'obliger l'utilisateur à changer de mot de passe au premier login et d'imposer un changement de mot de passe régulièrement.

Il existe 2 façons de modifier l'âge maximum du mot de passe :

La commande chage ou l'édition du fichier /etc/shadow

#### **Exemple chage :**

Obtenir les informations d'expiration :

**chage -l userName**





Chage exemple :

```
chage -M 60 -m 7 -W 7 userName
```

**/etc/shadow file format :**

```
{userName}:{password}:{lastpasswdchanged}:{Minimum_days}:{Maximum_d  
ays}:{Warn}:{Inactive}:{Expire}:
```

Lien pour faire configurer le changement de mot de passe au premier login.

<https://www.cyberciti.biz/faq/rhel-debian-force-users-to-change-passwords/>

Chercher tous les utilisateurs sans mot de passe pour les verrouiller :

<https://www.cyberciti.biz/tips/search-for-all-account-without-password-and-lock-them.html>

#### **Q. JOURNALISATION DES EVENEMENTS SERVEUR – DESKTOP**

La journalisation des évènements est essentielle. Elle peut d'autant plus être exportée vers le serveur qui centralisent les logs ou le SIEM du SOC.

La journalisation et l'exportation des logs se fera via Auditd

##### **Guide auditd Ubuntu Debian**

[https://linuxhint.com/auditd\\_linux\\_tutorial/](https://linuxhint.com/auditd_linux_tutorial/)

##### **Guide auditd CentOS RedHat**

<https://www.digitalocean.com/community/tutorials/how-to-use-the-linux-auditing-system-on-centos-7>

##### **Configuration des règles pour auditd valable pour tous les systèmes linux :**

Le responsable vous spécifiera les règles à appliquer

<https://github.com/Neo23x0/auditd/blob/master/audit.rules>

##### **Rotation des logs en local**

Il est recommandé de configurer la bonne rotation des logs selon le besoin.

Guide sur la rotation des logs

<https://www.cyberciti.biz/faq/how-do-i-rotate-log-files/>

#### **R. DESACTIVER IPV6 SI NON UTILISE SERVEUR – DESKTOP**



Si IPV6 n'est pas utilisé, il faut le désactiver, cela évitera l'exploitation de ce protocole.

Désactiver IPV6 sous RedHat, CentOS

<https://www.cyberciti.biz/faq/redhat-centos-disable-ipv6-networking/>

Désactiver IPV6 sous Debian, Ubuntu

<https://www.cyberciti.biz/tips/linux-how-to-disable-the-ipv6-protocol.html>

### S. TACHES PLANIFIEES – CRON **SERVEUR** – **DESKTOP**

Il est important de contrôler l'exécution des tâches planifiées. Une tâche planifiée est exécuté avec des privilèges élevés et peut induire des failles de sécurité.

D'abord il faut visualiser le fichier `/etc/crontab`

```
$ cat /etc/crontab
```

- Aucun des fichiers appelés ne doit être modifiable par un utilisateur sans privilège.
- Le path `/home/user` appelant la variable d'environnement ne doit pas être utilisé.
- Globalement, le caractère \* (wildcard) ne doit pas être utilisé dans un fichier appelé par cron ou dans cron.

Aucun des fichiers des répertoires suivant ne doit être modifiable par un utilisateur sans privilège.

- `/etc/cron.daily`
- `/etc/cron.weekly`
- `/ect/cron.monthly`

### T. CONTROLER LES PORTS EN ECOUTE SUR LE RESEAU **SERVEUR** – **DESKTOP**

Il peut être intéressant de contrôler les ports en écoute ou les connexions actives :

```
sudo lsof -i  
sudo netstat -lptu  
sudo netstat -tulpn
```

<https://www.cyberciti.biz/tips/linux-display-open-ports-owner.html>

On peut aussi utiliser ss ou nmap :

```
ss -tulpn
```

```
nmap -sT -O localhost
```



- ⚠ La partie scanner de vulnérabilité permettra d'avoir une visibilité complète sur les ports ouverts.

### U. DROITS SUR LES FICHIERS ET EXECUTABLES / FICHIERS SENSIBLES **SERVEUR** – **DESKTOP**

Les droits sur les fichiers ou les exécutable peuvent être exploités à des fins malveillantes et il convient de procéder à des vérifications les concernant :

Par convention, on évitera de base les droits de type **777** ou **rwX rwX rwX** qui induit que tout le monde a le droit en lecture écriture et exécution sur un fichier ou un exécutable.

#### 1 Droits sur les fichiers

##### Fichiers accessible à tous en écriture

Les fichiers accessibles à tous en écriture peuvent poser un problème pour la sécurité.  
Pour les référencer :

```
#find /dir -xdev -type d \( -perm -0002 -a ! -perm -1000 \) -print
```

Lien

<https://www.cyberciti.biz/faq/find-all-world-writable-directories-have-stickybitsset-on/>

##### Fichiers sans propriétaire

Les fichiers n'étant pas attribués à un utilisateur ou un groupe peuvent aussi poser un problème pour la sécurité :

```
#find /dir -xdev \( -nouser -o -nogroup \) -print-print
```

Il faudra investiguer tous les fichiers trouvés et réattribuer les droits le cas échéant si nécessaire

#### Droits sur les fichiers sensibles :

- ⚠ **/etc/shadow** et **/etc/passwd** ne doivent pas être accessible en écriture.  
**/etc/shadow** ne doit pas être accessible en lecture par un autre compte que root.

#### Fichiers sensibles :

Des fichiers peuvent être sensibles :

- Les fichiers « history » dans le path /home où un mot de passe en clair peut être stocké.  
accessibles via la commande

```
$ cat ~/.*history | less
```



- Les fichiers avec mot de passe ou clé souvent dans le repertoire /home
  - o Par exemple avec un fichier openvpn

```
$ ls -la /home/user
```

```
$ cat /home/user/myvpn/ovpn
```

- Les clés SSH  
Une clé SSH permet de se connecter en ssh. Si une clé se trouve être accessible, elle permettra une connexion directe sur la machine potentiellement avec un compte à privilèges élevés.

## 2 Droits sur les binaires :

setuid et setgid permettent d'exécuter des binaires avec les privilèges du détenteur du binaire. Cela permet à des utilisateurs non privilégiés d'accéder à des privilèges plus élevés dans certains cas comme une fonctionnalité d'un binaire dans un cas précis.

Exemple pour la commande « passwd » qui va permettre de modifier son mot de passe.

Un nombre important de binaires mal configurés sont à l'origine d'escalade de privilèges.

Plusieurs commandes permettent de voir les binaires avec toutes les bits activés et potentiellement exploitables :

Il faudra investiguer les fichiers qui remonteront :

```
#See all set user id files:
find / -perm +4000
# See all group id files
find / -perm +2000
# Or combine both in a single command
find / \( -perm -4000 -o -perm -2000 \) -print
find / -path -prune -o -type f -perm +6000 -ls
```

```
#See all executables on Debian :
find / -type f -a \( -perm -u+s -o -perm -g+s \) -exec ls -l {} \; 2> /dev/null
```

Plusieurs exploitables possible existent pour les binaires :

- Les exploits connus : <https://www.exploit-db.com/>
- L'injection dans les objets partagés (shared object injection)
- Variable d'environnement (user's path /usr/local/bin )



- Shell vulnérable (exemple Bash <4.2-048)

## V. CONFIGURER DES SAUVEGARDES **SERVEUR – DESKTOP**

Il est préconisé de configurer des sauvegardes du système, ces sauvegardes peuvent être effectuées en local sur un NAS ou sur le cloud type AWS.

L'entreprise utilise VEEAM pour ses assets importants :

**Guide pour déployer VEEAM via son agent :**

[https://helpcenter.veeam.com/docs/agentforlinux/userguide/installation\\_process.html?ver=50](https://helpcenter.veeam.com/docs/agentforlinux/userguide/installation_process.html?ver=50)

Il est aussi possible de configurer les sauvegardes sans VEEAM (pas de licence accordée):

**Configuration sauvegardes Debian Ubuntu**

<https://www.cyberciti.biz/faq/linux-rsnapshot-backup-howto/>

**Configuration sauvegardes RedHat Centos**

<https://www.cyberciti.biz/faq/linux-unix-apple-osx-bsd-rsync-copy-hard-links/>

## W. ENUMERATION GLOBALE VIA SCRIPT **SERVEUR – DESKTOP**

Il est préconisé de procéder à une énumération globale qu'on pourrait assimiler à un contrôle technique généralisé de différents points.

Les points remontés et mis en avant comme exploitables seront à corriger et permette de mettre l'accent sur des vulnérabilités ou des défauts de configuration.

**Différents scripts :**

<https://github.com/rebootuser/LinEnum/blob/master/LinEnum.sh>

<https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/blob/master/linPEAS/linpeas.sh>

## X. PARTAGES ET PROTOCOLE SAMBA (SMB) **SERVEUR – DESKTOP**

SMB porté sous linux avec SAMBA est vulnérables à différentes attaques.

Il peut parfois être activé par besoin ou par défaut comme sur les NAS.

Il est important de désactiver le SMB en version 1 dans tous les cas et de n'activer que les versions 2 ou 3 voire 3 et + uniquement.



Il faudra modifier le fichier /etc/samba/smb.conf et redémarrer le service

Un guide précise les modalités

<https://www.cyberciti.biz/faq/how-to-configure-samba-to-use-smbv2-and-disable-smbv1-on-linux-or-unix/>

## **Y. CHERCHER ROOTKITS – HARDENING TARDIF SERVEUR – DESKTOP**

En cas de doute sur une machine avec l'antivirus sophos et le hardening intervenant après la phase de déploiement initiale ou période de vulnérabilité connue.

Il est possible de vérifier l'existence d'un rootkit ( malware installé dans les couches basses qui est capable de se dissimuler)

Deux outils peuvent servir : chkrootkit et rkhunter.

Un guide détaille leur utilisation

<https://medium.com/@rkone1552000/rootkit-detection-chkrootkit-rkhunter-f52394116861>

## **Z. AUDIT AUTOMATISEE DES VULNERABILITES SERVEUR – DESKTOP**

La gestion des vulnérabilités est effectuée via la solution Qualys.

Il convient donc d'installer l'agent Qualys via le guide ci-dessous :

<https://www.qualys.com/docs/qualys-cloud-agent-linux-install-guide.pdf>

Le fichier pour installer l'agent correspondant à l'OS choisi vous sera fourni.

Un rapport des vulnérabilités sera disponible à l'issue des premiers scans.

## **AA. SOURCES**

<https://www.cyberciti.biz/tips/linux-security.html>

<https://github.com/trimstray/the-practical-linux-hardening-guide>

[https://linuxhint.com/linux\\_security\\_hardening\\_checklist/](https://linuxhint.com/linux_security_hardening_checklist/)

<https://madaidans-insecurities.github.io/guides/linux-hardening.html>

<https://www.pluralsight.com/blog/it-ops/linux-hardening-secure-server-checklist>

[https://www.ssi.gouv.fr/uploads/2016/01/linux\\_configuration-fr-v1.2.pdf](https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf)

<https://korben.info/crowdsec-fail2ban-liste-blocage-mutualisee.html>

<https://access.redhat.com/documentation/en->

[US/Red\\_Hat\\_Enterprise\\_Linux/7/html/Security\\_Guide/index.html](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/index.html)

<https://access.redhat.com/documentation/en->

[us/red\\_hat\\_enterprise\\_linux/7/html/selinux\\_users\\_and\\_administrators\\_guide/index](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/index)