UNIVERSITÉ LIBRE DE BRUXELLES

Configuration de base sécurisée pour GNU/LINUX

Version:	1.1
Date de la version:	11/02/2022
Créé par :	Alex GENATZY
Approuvé par :	CBA – C2i
Niveau de confidentialité :	Usage public

1 Comment maintenir votre GNU/LINUX sécurisé

Saviez-vous que même si votre GNU/Linux dispose des dernières mises à jour, l'anti-virus le plus récent et comporte un pare-feu (firewall), il peut malgré tout être infecté. Lorsque les ordinateurs sont utilisés de façon personnelle, plutôt que professionnelle, les risques d'infections ou d'autres incidents de sécurité augmentent (les films, jeux, musiques et autres applications personnelles entrainent tous des risques). Si vous gérez votre propre ordinateur ou installez vos propres applications, vous êtes aussi responsables de leur sécurité.

2 Utilisez une solution de sécurité pour les terminaux (antivirus) qui est automatiquement mise à jour

De nouveaux virus apparaissent quotidiennement. Les GNU/LINUX doivent être équipés d'une solution de sécurité (antivirus) automatiquement mise à jour afin de limiter les dommages des virus connus. Si un virus est découvert, la solution de sécurité (antivirus) vous le signalera, et l'empêchera de fonctionner (en le mettant en quarantaine).
Si vous installez la solution préconisée par l'ULB (« **Microsoft Defender for Endpoint »**), vous pourrez continuer de travailler normalement, le service support sera automatiquement informé et vous contactera si d'autres actions sont nécessaires.
Parfois, l'antivirus ne peut pas empêcher complètement les dommages, si vous rencontrez des problèmes, contactez **support@ulb.be** (tél: 3737), fournissez les détails du message d'erreur et du problème, et demandez une vérification complète de virus.

Toute personne gérant son propre PC est aussi responsable d'obtenir, d'installer et de mettre à jour son antivirus. Cela s'applique à tous les ordinateurs se connectant sur le réseau de l'ULB, y compris ceux des visiteurs. Le personnel de l'Université utilisant GNU/LINUX doivent utiliser la solution préconisée par l'institution « **Microsoft Defender for Endpoint** ». [1]
Alternativement, vous pouvez installer l'antivirus open source « **ClamAV** ».[2]

Sur un ordinateur personnel, les utilisateurs doivent installer une solution antivirus de leur choix.

Une solution de sécurité (antivirus) mise à jour régulièrement est particulièrement importante pour les GNU/LINUX qui sont utilisés dans divers endroits et connectés à d'autres fournisseurs d'accès à Internet, vu qu'ils évitent les protections de sécurité de l'Université.
Non seulement cela augmente leur risque d'infection, mais soumet le réseau ULB à des dangers, puisqu'une fois infectés, ils peuvent propager l'infection depuis l'intérieur du pare-feu de l'ULB.

3 Mettez à jour votre GNU/LINUX

La première chose à réaliser pour sécuriser votre GNU/LINUX est de mettre à jour les référentiels locaux et de mettre à niveau le système d'exploitation et les applications installées en appliquant les derniers correctifs.

Sur Ubuntu et Debian :

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

[1] https://support.ulb.be/group/support/-/comment-installer-et-executer-windows-defender-atp-sur-linux-fr
[2] http://www.clamav.net/

Sur Fedora, CentOS ou RHEL :

```
$ sudo dnf upgrade
```

Sur des anciennes versions de Fedora, CentOS ou RHEL :

```
$ sudo yum check-update
$ sudo yum update
```

Impact :
Sans mise à jour, votre système sera exposé à des risques supplémentaires.
Un logiciel non corrigé présente des vulnérabilités qui peuvent être exploitées.

3.1 Configure automated software patching – Configurer l'automatisation des correctifs logiciels

Certaines distributions peuvent automatiser les correctifs de sécurité. Bien qu'il existe un risque minimal d'indisponibilité d'un service, il l'emporte sur le risque d'une brèche de sécurité due à un logiciel vulnérable.

3.1.1 Utilisation de mises à niveau sur Debian et Ubuntu

Les vulnérabilités sont découvertes quotidiennement, ce qui nécessite également une surveillance quotidienne. L'application de correctifs logiciels prend du temps, en particulier lorsque des redémarrages sont nécessaires. Les systèmes exécutant Debian et Ubuntu peuvent utiliser des mises à niveau pour réaliser une gestion automatisée des correctifs pour les mises à jour de sécurité.

3.1.1.1 Installation

Avec la plupart des packages logiciels, des mises à niveau doivent être installées.
With most software packages, unattended-upgrades has to be installed.

```
$ sudo apt-get install unattended-upgrades
```

3.1.1.2 Configuration

Le fichier de configuration est nommé `/etc/apt/apt.conf.d/50unattended-upgrades`.
Par défaut, seules les mises à niveau de sécurité seront installées.
L'étape suivante consiste à configurer le package :
The configuration file is named `/etc/apt/apt.conf.d/50unattended-upgrades`
By default, only security upgrades will be installed.
Next step is to configure the package:

```
dpkg-reconfigure --priority=low unattended-upgrades
```

Sélectionnez que vous souhaitez installer des packages stables.
Select that you want to have stable packages installed.

3.1.2 Mises à jour de sécurité automatiques avec DNF

DNF : mises à jour de sécurité automatiques
L'outil DNF, est un gestionnaire de paquets pour les systèmes exécutant Fedora, CentOS 8 et RHEL 8. L'un des avantages de DNF est la possibilité de récupérer très facilement les informations de sécurité.

3.1.2.1 Security Patches - Correctifs de sécurité

Les versions plus récentes de Fedora utilisent DNF. The newer versions of Fedora use DNF

```
dnf updateinfo list security
```

Bien que cette sortie soit utile, nous voulons plus d'automatisation.
While this output is helpful, we want more automation

3.1.2.2 Install and Configure *dnf-automatic* - Installer et configurer *dnf-automatic*

Le package dnf-automatic simplifie la mise à jour automatique, en s'exécutant sur une minuterie, puis en appliquant les mises à jour. Vous pouvez le configurer pour simplement installer les mises à jour de sécurité.
The dnf-automatic package simplifies automatic patching, by running on a timer and then apply updates. You can configure it to just install security updates.

```
dnf install dnf-automatic
```

L'étape suivante pour appliquer uniquement les mises à jour de sécurité consiste à ajuster ce fichier `/etc/dnf/automatic.conf`. Configurez les paramètres suivants :
Next step to apply updates security updates only, is to adjust this `/etc/dnf/automatic.conf`. Configure the following settings:

```
apply_updates = yes
download_updates = yes
upgrade_type = security
```

Après avoir appliqué les modifications, vous avez terminé avec la partie configuration. Vérifiez maintenant l'état de la minuterie associée, pour voir si elle est activée.
After applying the changes, you are done with the configuration part. Now check the status of the related timer, to see if that is activated.

```
systemctl status dnf-automatic.timer
```

Cette minuterie est désactivée par défaut. Activez la minuterie et démarrez-la.
This timer will be disabled by default. Enable the timer and start it.

```
systemctl enable dnf-automatic.timer && systemctl start dnf-
automatic.timer
```

3.2 L'utilisation de logiciels non supportés (ou en fin de vie – « End of Life »).

Un logiciel qui n'est plus pris en charge est un logiciel en fin de vie. Pourtant, l'utilisation de ces logiciels en fin de vie et donc qui ne sont plus à jour présente des risques majeurs. Ils peuvent notamment contenir des failles qui vont menacer la sécurité d'un ordinateur ou les données personnelles de son utilisateur.
Pour vérifier, si vous utilisez des logiciels en fin de vie : **https://endoflife.date/**

- https://endoflife.date/linux

4 Lock Workstation Sessions After Inactivity – Verrouiller les sessions du poste de travail après une inactivité

Modifiez les fichiers `/etc/bash.bashrc, /etc/profile` et `/etc/profile.d/*.sh` (et les fichiers appropriés pour tout autre « shell » pris en charge sur votre système) et ajoutez ou modifiez le paramètre **TMOUT** : (1200 = 20 minutes)
Edit the `/etc/bash.bashrc`, `/etc/profile` and `/etc/profile.d/*.sh` files (and the appropriate files for any other « shell » supported on your system) and add or edit any **TMOUT** parameter :

```
readonly TMOUT=1200 ; export TMOUT
```

Remarque :
définir la valeur sur « readonly » empêche toute modification indésirable pendant l'exécution.
Note:
setting the value to « readonly » prevents unwanted modification during runtime

Impact:

- N'avoir aucune valeur de délai de pause associée à un shell pourrait permettre à un utilisateur non autorisé d'accéder à la session shell d'un autre utilisateur (par exemple, l'utilisateur s'éloigne de son ordinateur et ne verrouille pas l'écran.
- Having no timeout value associated with a shell could allow an unauthorized user access to another user's shell session (e.g. user walks away from their computer and doesn't lock the screen).

5 Security & Privacy - Sécurité et confidentialité

5.1 Encryption – Chiffrement

Si votre GNU/Linux dispose encore d'un Disque Dur (Hard Disk), nous vous recommandons de remplacer votre HDD pour Hard Drive Disk (ou disque dur mécanique) par un SSD pour Solid State Drive (ou disque à mémoire flash). Notre Atelier Informatique peut vous assister pour cette opération :

https://atelierinformatique.ulb.be/

5.1.1 How to Encrypt Storage Drives Using LUKS in Linux – Comment chiffrer les disques de stockage à l'aide de LUKS sous Linux

Pendant le chiffrement, LUKS « Linux Unified Key Setup » réserve un espace sur le lecteur de stockage et stocke les informations nécessaires requises pour le chiffrement et le déchiffrement sur le lecteur de stockage lui-même. Cette méthodologie de chiffrement sur disque garantit une compatibilité quasi plug and play entre les distributions Linux et une transférabilité aisée des lecteurs de données. Tant que LUKS est installé sur votre système Linux et que vous connaissez le mot de passe, vous pourrez facilement déchiffrer n'importe quel lecteur de données chiffré LUKS sur n'importe quelle distribution Linux.

During encryption, LUKS « Linux Unified Key Setup » reserves a space on the storage drive and stores necessary information required for encryption and decryption on the storage drive itself. This on-disk encryption methodology ensures near plug and play compatibility across Linux distributions and easy transferability of data drives. As long as you have LUKS installed on your

Linux system and you know the password, you will be easily able to decrypt any LUKS encrypted data drive on any Linux distribution.

5.1.1.1 Installing LUKS - Installation de LUKS

LUKS fait partie du package « cryptsetup », vous pouvez l'installer dans Debian, Ubuntu en exécutant la commande ci-dessous :
LUKS is a part of the « cryptsetup » package, you can install it in Debian, Ubuntu by running the command below:

```
$ sudo apt install cryptsetup
```

Vous pouvez installer « cryptsetup » sur Fedora en exécutant la commande ci-dessous :
You can install « cryptsetup » on Fedora by running the command below:

```
$ sudo dnf install cryptsetup-luks
```

5.1.1.2 How to encrypt with LUKS – Comment chiffrer avec LUKS

- FR : https://wiki.evolix.org/HowtoLUKS
- UK : https://gitlab.com/cryptsetup/cryptsetup/-/wikis/home

5.1.2 Chiffrement alternatif pour notamment vos lecteurs réseaux (« cryptomator»)

La seule tâche de « **Cryptomator** » est le chiffrement. « **Cryptomator** » est un outil qui chiffre vos fichiers et vous permet de les synchroniser entre les périphériques via le cloud ou les lecteurs USB en toute sécurité. Ceci est très utile lorsque vous travaillez avec des informations privées et/ou sensibles, car il vous permet de chiffrer vos informations (les rendre illisibles) pour qu'elles ne soient consultées que lorsque vous le souhaitez et de les synchroniser sur vos différents appareils.
Installation et documentation:

- **Dépôt :** https://cryptomator.org/downloads/
- **Références** : https://docs.cryptomator.org/en/latest/

5.1.3 Chiffrement alternatif du système d'exploitation (« VeraCrypt »)

Vous pouvez utiliser « **VeraCrypt** », un logiciel open-source et gratuit de chiffrement de données. « **VeraCrypt** » permet de chiffrer et déchiffrer les données à la volée, c'est-à-dire de manière transparente pour l'utilisateur et le système. Vous pouvez utiliser « **VeraCrypt** » pour chiffrer un fichier, une partition de disque ou l'ensemble d'un disque dur.

- **Dépôt :** https://www.veracrypt.fr/code/VeraCrypt
- **Références** : Chiffrement du disque d'un support de stockage à l'aide de « **VeraCrypt** » https://www.veracrypt.fr/en/Home.html

Installez « **VeraCrypt** »

1. Allez sur le site officiel de et téléchargez la dernière version de « **VeraCrypt** » pour Windows.
2. Effectuez l'installation en gardant les options par défaut et choisissez *Français* pour la langue d'installation.

À la fin de l'installation, « **VeraCrypt** » vous propose de lire la documentation (en anglais). Cette documentation est très complète et vous pourrez l'utiliser par la suite pour aller plus loin dans l'utilisation de « **VeraCrypt** ».

5.2 Enable Firewall - Activer le pare-feu

5.2.1 Pour Debian et la plupart des autres distributions

Pour Debian et la plupart des autres distributions, **firewalld** peut être installé à partir de votre référentiel de logiciels. Pour utiliser **firewalld**, donc, vous devez activer le référentiel d' « universe »:
On Debian and most other distributions, **firewalld** is available to install from your software repository. To use **firewalld**, you must enable the « universe » repository:

```
$ sudo add-apt-repository universe
$ sudo apt install firewalld
```

5.2.2 Pour les distributions Fedora Linux/CentOS/RHEL

Pour les Linux Fedora Linux/CentOS/RHEL et les distributions similaires, le logiciel de pare-feu installé par défaut est **firewalld**, qui est configuré et contrôlé avec la commande firewall-cmd.
On Fedora, CentOS, Red Hat, and similar distributions, the firewall software installed by default is **firewalld**, which is configured and controlled with the firewall-cmd command.

5.2.3 Active at boot time - Activation dès le démarrage

Quelle que soit votre distribution, pour que votre pare-feu soit efficace, il doit être actif, et il doit être chargé au démarrage :
Regardless of your distribution, for a firewall to be effective, it must be active, and it should be loaded at boot time:

```
$ sudo systemctl enable --now firewalld
```

Impact:

- The firewall may block legitimate traffic.
- Le pare-feu peut bloquer le trafic légitime.

6 Create backups and check restores – Créer des sauvegardes et vérifier les restaurations

Avant toute chose, sachez qu'il est vivement recommandé d'investir dans un disque dur externe compatible pour GNU/LINUX. Idéalement, la capacité de stockage de ce disque dur externe doit être +/- 2 fois la taille de votre disque interne.

Surtout après l'installation, assurez-vous que votre sauvegarde fonctionne. Vérifiez vos sauvegardes en effectuant des tests de restauration.
Especially after the installation, make sure your backup is working. Check your backups by performing test restores.

The best Linux Backup Solutions – Les meilleures solutions de sauvegarde Linux :
https://linuxsecurity.com/best-linux-backup-solutions

6.1 How to back up a Linux system with Timeshift – Comment sauvegarder un système Linux avec Timeshift

Timeshift est disponible dans presque tous les référentiels de distribution..
https://github.com/teejee2008/timeshift/blob/master/README.md

Pour installer Timeshift sur un système Debian, utilisez la commande :
To install Timeshift on an Ubuntu system, use the command:

```
$ sudo apt install timeshift
```

Pour installer Timeshift sur un système Fedora, utilisez la commande :
To install Timeshift on a Fedora system, use the command:

```
$ sudo dnf install timeshift
```

Pour installer Timeshift sur un système RedHat, utilisez la commande :
To install Timeshift on a RedHat system, use the command:

```
$ sudo yum install timeshift
```

7 File System Permissions and Access Controls - Autorisations du système de fichiers et contrôles d'accès

7.1 Secure Home Folders - Dossiers personnels sécurisés

Remediation - Remédiation:
Pour chaque utilisateur, exécutez la commande suivante pour sécuriser tous les dossiers personnels:
For each user, run the following command to secure all home folders:

```
$ sudo chmod -R og-rwx /home/<username>
```

Sinon, exécutez la commande suivante si un accès « exécutable » pour un dossier personnel est nécessaire:
Alternately, run the following command if there needs to be executable access for a home folder:

```
$ sudo chmod -R og-rw /home/<username>
```

8 Password Management - Gestion mots de passe

Les bonnes pratiques:

- Votre mot de passe doit rester personnel, pas de mot de passe partagé entre plusieurs utilisateurs.
- Votre mot de passe doit être suffisamment complexe (utilisation d'un mélange de lettres, ***majuscules, minuscules, chiffres*** et idéalement des caractères de ponctuation) d'une longueur ***minimum de 15 caractères***.
- Votre mot de passe doit être changé assez régulièrement
- Votre mot de passe doit être changé dès que vous en soupçonnez sa compromission (vol ou perte du PC, divulgation à un tiers, etc.)

8.1 Complex passwords must uppercase and lowercase letters - Les mots de passe complexes doivent être majuscules et minuscules

Le module **`pam_pwquality.so`** vérifie la force des mots de passe. Il effectue des vérifications telles que s'assurer qu'un mot de passe n'est pas un mot du dictionnaire, qu'il a une certaine longueur, qu'il contient un mélange de caractères (par exemple, alphabet, numérique, autre) et plus encore.

Les options suivantes sont définies dans le fichier **`/etc/security/pwquality.conf`** :

Longueur du mot de passe:

- **minlen** = 15
  - le mot de passe doit comporter 15 caractères ou plus
  - password must be 15 characters or more

Nombre de tentatives infructueuses :

- **retry** = 3
  - Autorisez 3 essais avant de renvoyer un échec.
  - Allow 3 tries before sending back a failure.

Complexité du mot de passe :

- **minclass** = 4
  - Le nombre minimum de classes de caractères requises pour le nouveau mot de passe (chiffres, majuscules, minuscules, autres)
  - The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others)

OU

- **dcredit** = -1
  - au moins un chiffre
  - at least one digit
- **ucredit** = -1
  - au moins un caractère majuscule
  - at least one uppercase character
- **ocredit** = -1
  - au moins un caractère spécial
  - at least one special character
- **lcredit** = -1
  - au moins un caractère minuscule
  - at least one lowercase character

Remediation :
Exécutez la commande suivante pour installer le module `pam_pwquality`:
Run the following command to install the `pam_pwquality` module:

Pour Debian et la plupart des autres distributions

```
$ sudo apt install libpam-pwquality libpwquality-tools
```

8.2 Conservez vos mots de passe en lieu sûr

Mémoriser plusieurs mots de passe peut être difficile. Afin d'éviter de les oublier, conservez la liste de vos mots de passe hors connexion en un lieu sûr, secret et verrouillé. Ne la conservez pas dans votre boîte de messagerie ou ailleurs en ligne.

8.2.1 Gestionnaire de phrases et mots de passe

Si vous êtes dépassé par le nombre de mots de passe que vous devez retenir, vous pouvez utiliser un gestionnaire de mots de passe pour les générer et les conserver. Les mesures suivantes peuvent vous aider à protéger les mots de passe stockés dans un gestionnaire de phrases et mots de passe :

- Stockez uniquement les mots de passe associés à vos comptes qui ne nécessitent pas des privilèges administratifs ou des justificatifs d'identité liés à des comptes bancaires.

- Utilisez un mot de passe robuste et une authentification à deux facteurs pour sécuriser votre gestionnaire de mots de passe.

Nous vous recommandons le gestionnaire de mot de passe suivant :
« **Bitwarden** »: https://bitwarden.com/

9 « root » account - compte « root »

Ne vous connectez pas en tant que **root**. La connexion en tant que **root** signifie que vous naviguerez sur Internet en tant que **root**, que vous effectuerez des téléchargements, les scripts malveillants peuvent désormais tous s'exécuter avec les permissions **root**.
Don't Log in as **root**. Logging in as **root** means you will be browsing the Internet as **root**, drive by downloads, malicious scripts can all now execute with **root** permission.

9.1 Ensure **root** is the only UID 0 account – Assurez-vous que **root** est le seul compte UID 0

Cet accès doit être limité uniquement au compte **root** par défaut et uniquement à partir de la console système. L'accès administratif doit se faire via un compte non privilégié à l'aide d'un mécanisme approuvé, comme indiqué dans la recommandation « Assurez-vous que l'accès à la commande **« su »** est restreint ».
This access must be limited to only the default **root** account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in recommendation « Ensure access to the **« su »** command is restricted».

```
$ awk -F: '($3 == 0) { print $1 }' /etc/passwd
```

Remediation :
Supprimez tous les utilisateurs autres que **root** avec l'UID **0** ou attribuez-leur un nouvel UID, le cas échéant.
Remove any users other than **root** with UID **0** or assign them a new UID if appropriate.

9.2 Ensure default group for the **root** account is GID 0 – Assurez-vous que le groupe par défaut pour le compte **root** est GID 0

L'utilisation de GID 0 pour le compte **root** permet d'éviter que les fichiers appartenant à **root** ne deviennent accidentellement accessibles aux utilisateurs non privilégiés.
Using GID 0 for the **root** account helps prevent **root**-owned files from accidentally becoming accessible to non-privileged users.

```
$ grep "^root:" /etc/passwd | cut -f4 -d:
```

Remediation:
Exécutez la commande suivante pour définir le groupe par défaut de l'utilisateur **root** sur GID **0** :
Run the following command to set the **root** user default group to GID **0** :

```
$ usermod -g 0 root
```

10 Disable Automounting – Désactiver le montage automatique

Objectif :
Les supports amovibles comprennent les clés USB, les cartes mémoire et les disques durs externes - pour ne citer que quelques exemples. Ces appareils sont souvent utilisés pour stocker des photos, des vidéos et de nombreux types de données. Les supports amovibles sont également utilisés par les attaquants pour installer des logiciels malveillants sur les systèmes informatiques. Cette méthode d'attaque peut être utilisée pour infecter les postes de travail, mais aussi les systèmes informatiques considérés comme sécurisés car dépourvus de connexion WiFi ou Internet. Si le logiciel sur un périphérique USB est autorisé à s'exécuter automatiquement, il peut être en mesure d'installer des logiciels malveillants avec une interaction limitée ou nulle de l'utilisateur.

Purpose:
Removable media includes USB drives, memory cards, and external hard drives - just to name a few examples. These devices are used to store photos, videos, and many types of data. Removable media is also one method used by attackers to install malicious software on computer systems. This attack method can be used to infect workstations, but also computer systems viewed as secure since they lack a WiFi or Internet connection. If software on a USB device is allowed to automatically run, it may be able to install malware with limited to no user interaction.

- **`autofs`** permet le montage automatique de périphériques, notamment des CD/DVD et des clés USB.
- **`autofs`** allows automatic mounting of devices, typically including CD/DVDs and USB drives.

- **`autofs`** doit être supprimé ou désactivé.
  `autofs` should be removed or disabled
  `$ systemctl is-enabled autofs`
  Vérifiez que le résultat n'est pas « activé ».
  Verify result is not « enabled ».

  OU Exécutez la commande suivante pour vérifier que **`autofs`** n'est pas installé
  OR Run the following command to verify that **`autofs`** is not installed
  `$ dpkg -s autofs`

11 Ne téléchargez pas, n'installez pas et n'exécutez pas de logiciels depuis des sources « non sures »

Parmi ces sources exposées au danger :

- Internet,
- les clés USB,
- CDs, DVDs,
- etc. ...

Un nombre croissant d'incidents de sécurité informatique détectés à l'ULB est dû à des logiciels téléchargés, installés ou exécutés depuis des sources douteuses. Lorsque vous copiez et exécutez un fichier contenant un virus, vous pouvez non seulement infecter votre propre ordinateur, mais également commencer à propager un virus à l'intérieur du réseau ULB en contournant le pare-feu (firewall).

Les « **Logiciels gratuits** » populaires disponibles sur le Web peuvent introduire des problèmes de sécurité, soit lorsque le logiciel est installé (par exemple en installant des logiciels espions (« spyware ») ou plus tard, à cause du manque de mises à jour servant à éliminer les failles de sécurité. De plus l'installation d'un module d'extension (en anglais « plug-in ») peut aussi télécharger un logiciel malicieux que l'extension peut contenir. Si un site web nécessite un « plug-in » pour être visualisé, il vaut mieux ne pas l'activer.

En plus des problèmes de sécurité, les logiciels installés pour une utilisation personnelle créent souvent des problèmes de support. Les logiciels additionnels peuvent rendre l'analyse des problèmes plus difficile (temps de résolution plus grand).

Pour télécharger/installer vos logiciels, veuillez-vous référer à nos recommandations:

- Installez vos apps de GNU/Linux https://github.com/Linuxbrew/legacy-linuxbrew

12 Références

- **CIS** - Center For Internet Security CIS - GNU/LINUX Benchmark

https://downloads.cisecurity.org/?bypassToken=zrcxFuY5xcKHFXEhL6ffC5hNpKnOlj6f#/

- **ANSSI** - Agence nationale de la sécurité des systèmes d'information

https://www.ssi.gouv.fr/administration/bonnes-pratiques/

- **@trimstray**

https://github.com/trimstray/linux-hardening-checklist

- **Linux and Unix security solutions**

https://cisofy.com/checklist/linux-security/

- **Basic Ubuntu Security Guide, Desktop Edition**

https://wiki.ubuntu.com/BasicSecurity