LE GUIDE DE SECURISATION POUR UBUNTU 14.04

v1.4

Ce guide a pour but d'aider à l'installation d'un système GNU/Linux qui soit sécurisé et utilisable dans les activités de tous les jours (web, vidéo, divertissement, musique etc)

Pour les activités extrêmement sensibles (deep, fraude, criminalité) il ne faut pas utiliser son système qui est dédié aux activités journalières. Vous devez utiliser TAILS ou une machine virtuelle. (je reviendrais peut être sur ce sujet)

J'ai choisi Ubuntu 14.04 pour ce tuto mais vous pouvez aussi l'appliquer sur Debian, Ubuntu 12.04 (mais il risque d'y avoir des différences logicielles) et d'autres distributions comme Xubuntu, Kubuntu mais les logiciels cités dans ce tuto peuvent être absents ou différents ! (je n'ai pas testé sur Arch)

Ubuntu est bon système d'exploitation, il est sûr, stable, complet, facile d'utilisation, beau, pas très gourmand. Sauf qu'il vient par défaut avec une multitudes de programmes dangereux qui ne servent à rien.

Nous allons voir de A à Z comment installer et configurer Ubuntu, cette installation est légèrement différente si vous souhaitez un dual-boot avec Windows (ça peut toujours servir). De plus je dois aussi mettre la partie concernant les systèmes UEFI (le nouveau Bios) car l'installation diffère là aussi. Je suis obligé de mettre les UEFI car les nouveaux PC sont tous équipés de ce nouveau Bios.

N'hésitez absolument pas à faire des remarques, si il manque un truc ou si vous pensez qu'il y'a une erreur. Aucun tutoriel n'est parfait, il peut manquer des informations ou des modifications, j'ai essayé de montrer les modifications essentielles mais il doit en rester sûrement d'autres. Dites moi les modifications que vous pensez nécessaires et je les rajouterais avec plaisir en mentionnant votre nom.

Ce guide est la procédure que j'applique systématiquement à tout système GNU/Linux que j'installe fraîchement sur mon ordinateur. Jusqu'à présent je n'ai rencontré aucun problème mais ce n'est pas parce que je n'ai pas de problème que vous n'en rencontrerez pas aussi ! (matériel différent, etc)

Je vous conseille fortement de tester toute la manipulation de A à Z dans une machine virtuelle (y compris le dual-boot avec windows) pour ne pas faire d'erreur.

N'oubliez pas de sauvegarder vos fichiers avant toutes manipulations. VOUS ETES PREVENUS.

UBUNTU SEUL (non-UEFI)

1] Télécharger Ubuntu

- Suivant votre système : 32 bits ou 64 bits http://www.ubuntu.com/download/desktop/

2] Installer Ubuntu sur une clé USB

- Rien de plus facile http://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/
- Sous Linux, utilisez le programme Unetbootin.

3] Booter sur sa clé USB

- Insérez votre USB
- Démarrez votre PC
- Lors du démarrage appuyez sur F12, Echap, F9 ou F10 pour avoir les options d'amorçage
- Bootez sur votre USB

4] Essayer toujours Ubuntu avant de l'installer

- Vérifier que votre matériel est bien reconnu dans « About this computer » en haut à droite.
- Dans les réglages du langage ajoutez le Français pour passer le clavier en azerty.

5] Choisir son mot de passe pour le Full Disk Encryption (FDE)

C'est une étape très importante, ne négligez JAMAIS la robustesse de votre mot de passe.

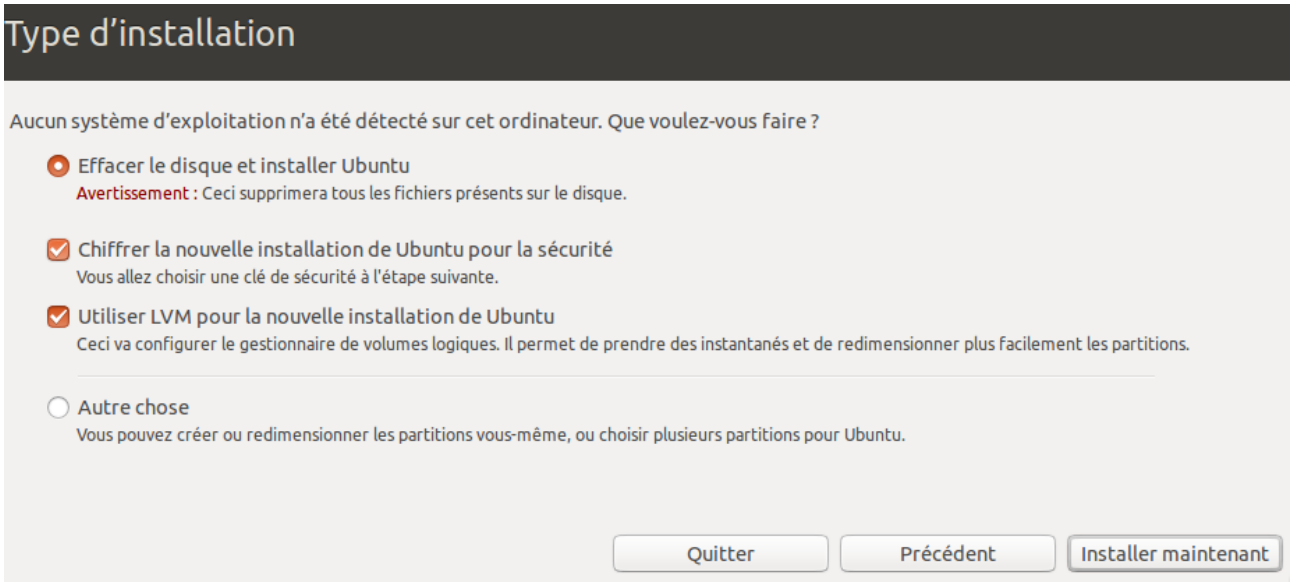
Votre mot de passe de chiffrement doit :
- faire au strict minimum 30 caractères
- comporter des lettres minuscules, majuscules, des chiffres et caractères spéciaux
- ne doit pas être sensible à une attaque dictionnaire (évitez les citations à la lettre)
- ne doit jamais être écrit sur un support physique, ni virtuel
- ne doit jamais être divulguée
- ne doit jamais être écrit sur une machine susceptible d'être compromise

Je donnerais plus loin les consignes de sécurité qu'il faut scrupuleusement respecter pour garantir la confidentialité de votre mot de passe et par la même occasion votre système.

Maintenant :
- Ouvrez un éditeur texte : Gedit
- Écrivez votre mot de passe, attention aux espaces à la fin et au début
- Copiez-collez votre mot de passe

6] Démarrer l'installation

- Lancez l'installation, ne cochez pas les cases de mise à jour et des «Logiciels tiers »
- Cochez les 3 premières cases et cliquez sur installer.
- Si vous avez Windows, n'installez pas Ubuntu à côté
- Effacez le disque et installez Ubuntu à la place de windows (en cochant les cases de chiffrement)



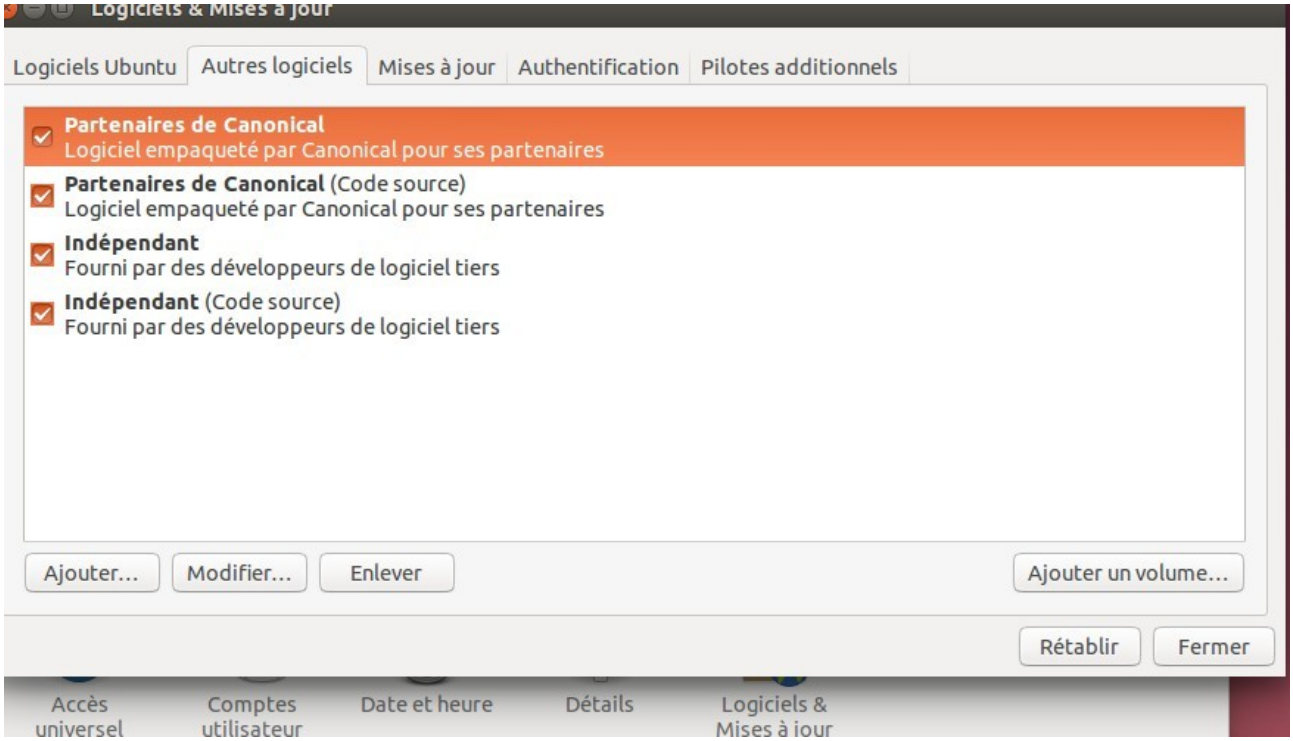
- Collez votre mot de passe de chiffrement puis continuez.
- Continuez l'installation jusqu'à la fin puis redémarrez.

Vous devrez rentrer votre mot de passe de chiffrement. Si rien ne s'affiche appuyez sur F1 pour afficher la ligne dans laquelle vous devez taper votre mot de passe.

7] Activez les sources de logiciels supplémentaires :

Dans Paramètre Système ---> Logiciel & Mises à jour

Activez les Partenaires de Canonical pour avoir une plus grande liste de logiciel disponible.



Je vous conseille de ne pas installer les pilotes additionnels pour prendre en charge la carte graphique. Si le système s'affiche correctement, si il n'y pas de problème, n'installez pas les drivers Nvidia/AMD.

Sauf si vous en avez vraiment besoin, dans ce cas FAITES D'ABORD LES MISES A JOURS et installez ensuite les drivers. Car le noyau Linux sera mis à jour et lors de chaque mise à jour du noyau les drivers propriétaires doivent être réinstallés.

8] Désinstaller les programmes inutiles (et dangereux)

Ubuntu vient par défaut avec des programmes qui ne servent strictement à rien, non seulement ils ne servent à rien (pour les personnes paranoïaques que nous sommes) mais ce genre de programme peut compromettre la sécurité du système. Les développeurs d'Ubuntu devraient sérieusement revoir leur monture au lieu de nous donner Ubuntu avec ces merdes pré-installées.

- Dans un terminal tapez « sudo apt-get install synaptic » et installez le gestionnaire de paquets
- Lancez Synaptic via le lanceur rapide (en haut à gauche)

Supprimez complètement les programmes suivants :

- Xterm
- deja-dup + deja-dup-backend-gvfs (séléctionnez les 2 paquets avec CTRL pour une suppression complète)
- gnome-orca

Écrivez dans la barre de recherche « unity» et supprimez complètement les paquets suivants

- unity-lens-friends
- unity-lens-photos
- unity-scope-audacious
- unity-scope-chromiumbookmarks
- unity-scope-clementine
- unity-cope-colourlovers
- unity-scope-devhelp
- unity-scope-firefoxbookmarks
- unity-scope-gdrive
- unity-scope-gmusicbrowser
- unity-scope-gourmet
- unity-scope-guayadeque
- unity-scope-musicstores
- unity-scope-musique
- unity-scope-openclipart
- unity-scope-texdoc
- unity-scope-tomboy
- unity-scope-video-remote
- unity-scope-virtualbox
- unity-scope-zotero

Ensuite, supprimez intégralement les paquets :

- shotwell et shotwell-comon
- remmina, remmina-common, remmina-plugin-rdp et remmina-plugin-vnc

Ensuite, écrivez « firefox » dans la barre de recherche et supprimez intégralement :

- firefox
- rhytmbox-mozilla
- xul-ext-ubufox
- firefox-locale-en
- libufe-xidgetter0
- totem-mozilla
- webaccounts-extension-common
- xul-ext-unity
- xul-ext-webaccounts
- xul-ext-websites-integration

Oui on supprime Firefox et toutes les merdes associées pour pouvoir le réinstaller proprement plus tard. Pas d'inquiétude.

Ensuite, supprimez intégralement le paquets :

- webbrowser-app

Vous aurez une notification qui vous dira que d'autres paquets seront aussi supprimés, acceptez. Les paquets qui seront aussi supprimés avec le paquet « webbrowser-app » sont :

- libunity-webapps0
- unity-webapps-common
- unity-webapps-service
- webapp-container

Ensuite supprimez complètement les paquets :

- unity-webapps-qml
- vino

Maintenant à moins d'utiliser explicitement Thunderbird car vous recevez vos courriels sur Ubuntu il vaut mieux supprimer Thunderbird. Ceux qui utilisent Thunderbird peuvent passer cette étape.

Supprimez seulement si vous ne les utilisez pas les paquets suivants :

- thunderbird
- thunderbird-gnome-support
- thunderbird-locale-en
- thunderbird-locale-en-us
- thunderbird-locale-fr

Si vous utilisez des messageries instantanées pour discuter avec des amis, je vous conseille de suivre les conseils présents dans ce tutoriel. Nous allons supprimer Empathy, un client de discussion qui doit être remplacé par Pidgin (si vous souhaitez discuter avec des amis).

Écrivez « Empathy » dans la barre de recherche et supprimez intégralement :

- account-plugin-aim
- account-plugin-jabber
- account-plugin-salut
- account-plugin-yahoo
- empathy
- empathy-common
- nautilus-sendto-empathy
- gnome-contacts
- telepathy-idle

Une notification vous indiquera que le paquet « mcp-account-manager-uoa » sera aussi supprimé. Acceptez.

Ensuite supprimez intégralement les paquets :

- transmission-common
- transmission-gtk

C'est un client bittorrent, remplacez le plus tard par Qbittorrent qui est largement mieux.

Ensuite écrivez dans la recherche « totem » et supprimez intégralement :

- gir1.2-totem-1.0
- gir1.2-totem-plparser-1.0
- libtotem0
- totem
- totem-common
- totem-plugins

Aucun lecteur multimédia ne peut arriver à la cheville de VLC Media Player. Installez VLC quand vous aurez fini l'installation.

Écrivez ensuite « rhythmbox » dans la barre de recherche puis supprimez intégralement :

- rhythmbox

Une notification vous indiquera que les paquets suivants seront aussi supprimés (acceptez) :

- rhythmbox-plugin-cdrecorder
- rhythmbox-plugin-magnatune
- rhythmbox-plugin-zeitgeist
- rhythmbox-plugins

Puis supprimez les paquets suivants :

- gir1.2-rb-3.0
- librhythmbox-core8
- rhythmbox-data

Rhythmbox est un lecteur de musique lourd, VLC remplit parfaitement son rôle pour lire la musique et faire des playlists, en plus il est bien intégré dans Ubuntu. Au pire vous pouvez installer Audacious comme lecteur de musique.

Ensuite supprimez intégralement les paquets suivants :

- gnome-user-share
- landscape-client-ui-install
- unity-control-center-signon

Ensuite écrivez « account » dans la barre de recherche et supprimez intégralement :

- account-plugin-facebook
- account-plugin-flickr
- account-plugin-google
- account-plugin-twitter
- account-plugin-windows-live

Une notification vous indiquera que les paquets « friends-facebook » et « friends-twitter » seront aussi supprimés, acceptez et désinstallez ces saloperies.

Toujours dans la même liste, supprimez intégralement :

- libaccount-plugin-google
- qtdeclarative5-accounts-plugin
- telepathy-mission-control-5

Sélectionnez simultanément les paquets suivants et supprimez-les :

- libgoa-1.0-0b
- libgoa-1.0-common
- libmission-control-plugins0

Une notification vous indiquera que ces paquets seront aussi supprimés (acceptez) :

- evolution-data-server
- evolution-data-server-online-accounts
- gir1.2-gdata-0.0
- gir1.2-goa-1.0
- libfolks-eds25
- libgdata13

Ensuite supprimez le paquet :

- folks-common

Une notification vous indique que les paquets suivants seront aussi supprimés (acceptez)

- libfolks-telepathy25
- libfolks25

Ensuite écrivez « telepathy » dans la barre de recherche puis supprimez intégralement le paquet :

- libtelepathy-glib0

Une notification vous indique que les paquets suivants seront supprimés (acceptez) :

- libtelepathy-farstream3
- libtelepathy-logger3
- telepathy-gabble
- telepathy-haze
- telepathy-indicator
- telepathy-logger
- telepathy-salut
- zeitgeist
- zeitgeist-datahub

Ensuite supprimez intégralement le paquet :

- libpurple0

Ensuite écrivez « friend » dans la barre de recherche, sélectionnez simultanément puis supprimez les paquets :

- friends
- friends-dispatcher
- libfriends0

Redémarrez Ubuntu.

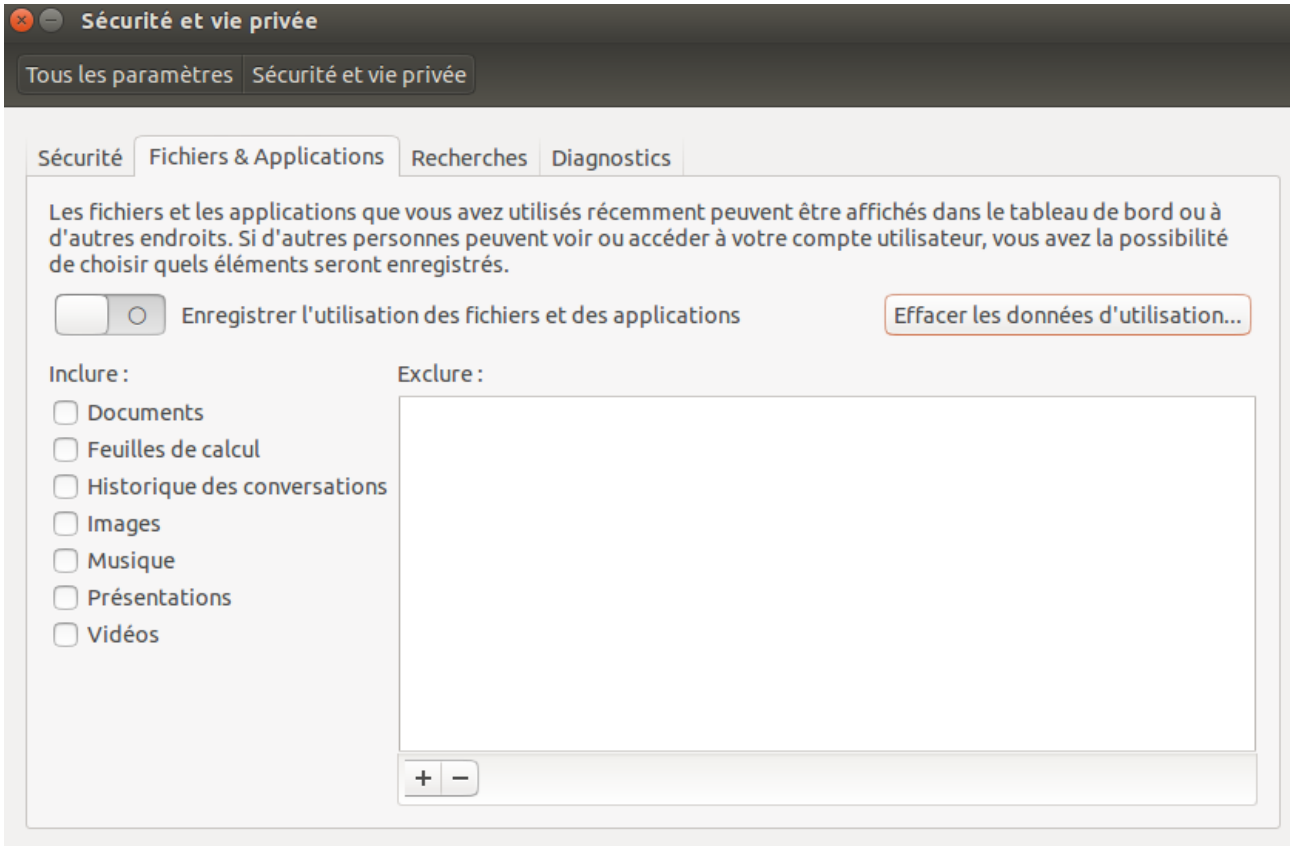
Faites les mises à jour

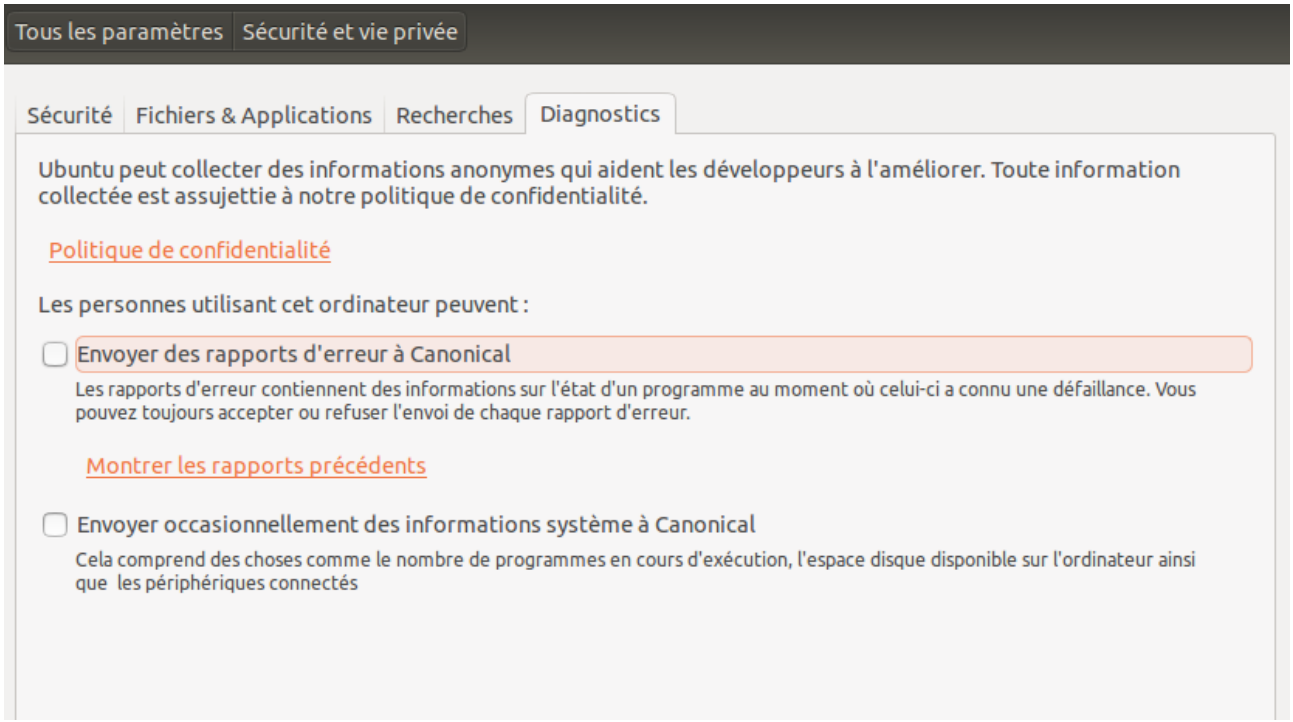
Puis redémarrez à nouveau.

9] Régler les paramètres de vie privée

Dans les paramètres système, ouvrez l'onglet « Sécurité et vie privée »

- Désactivez l'enregistrement de l'historique des fichiers et applications.
- Désactivez les recherches en ligne
- Désactivez les rapports d'erreur et de diagnostic





Ensuite, ouvrez un terminal et copiez-collez (à ne faire que sous Ubuntu unity)

- wget -q -O - https://fixubuntu.com/fixubuntu.sh | bash

C'est un script qui va complètement désactiver les recherches personnalisées avec les services en ligne (amazon).

Le script provient de https://fixubuntu.com/

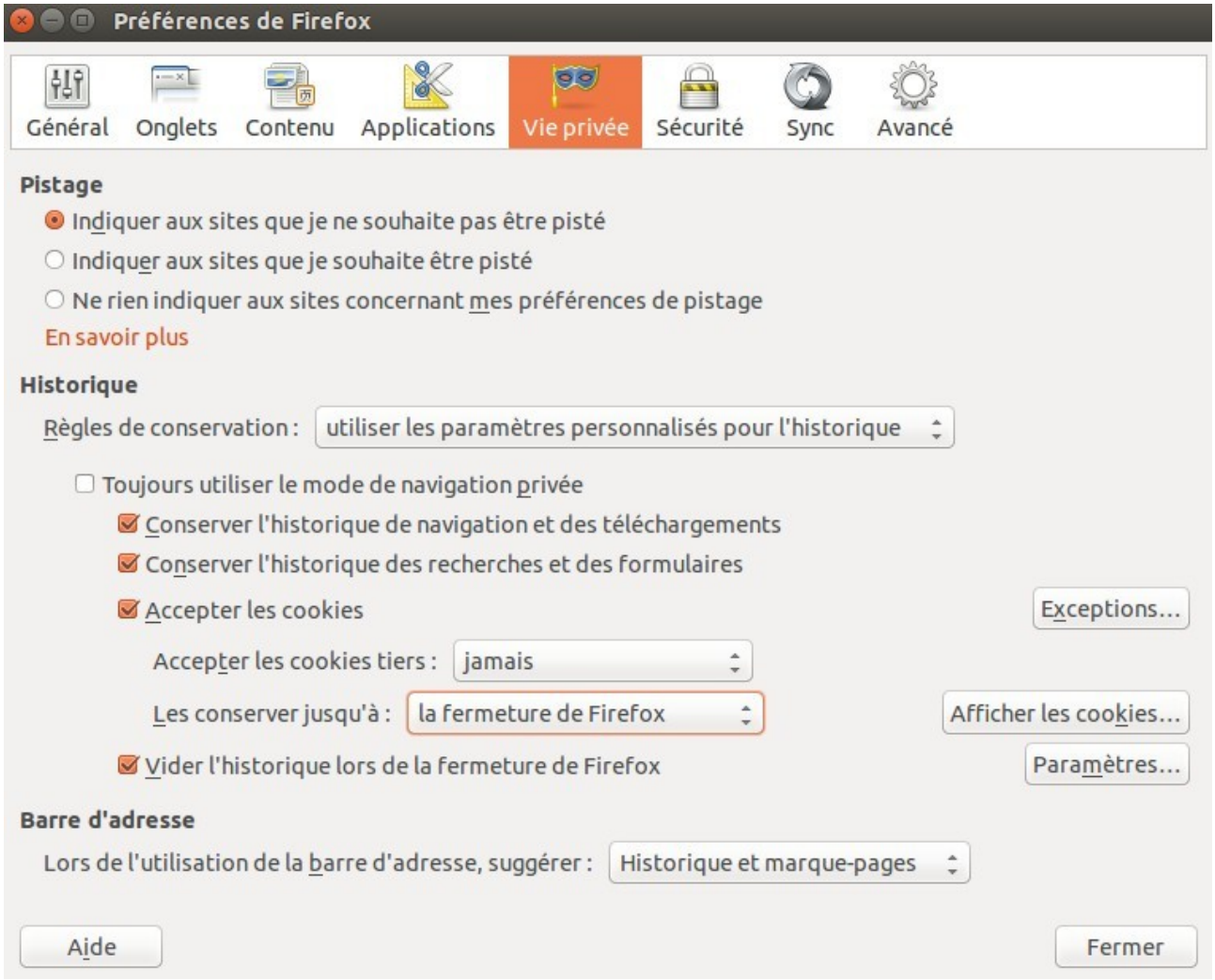
10] Installer Firefox et les modules indispensables

- Ouvrez le gestionnaire de paquets Synaptic et installez Firefox.
- Une fois l'installation terminée, vous devez supprimer le paquet « xul-ext-ubufox ».
- Installez le paquet « adobe-flashplugin » si vous voulez accéder aux vidéos sur la plupart des sites web (il faut de toute urgence un remplaçant libre pour cette usine à gaz)

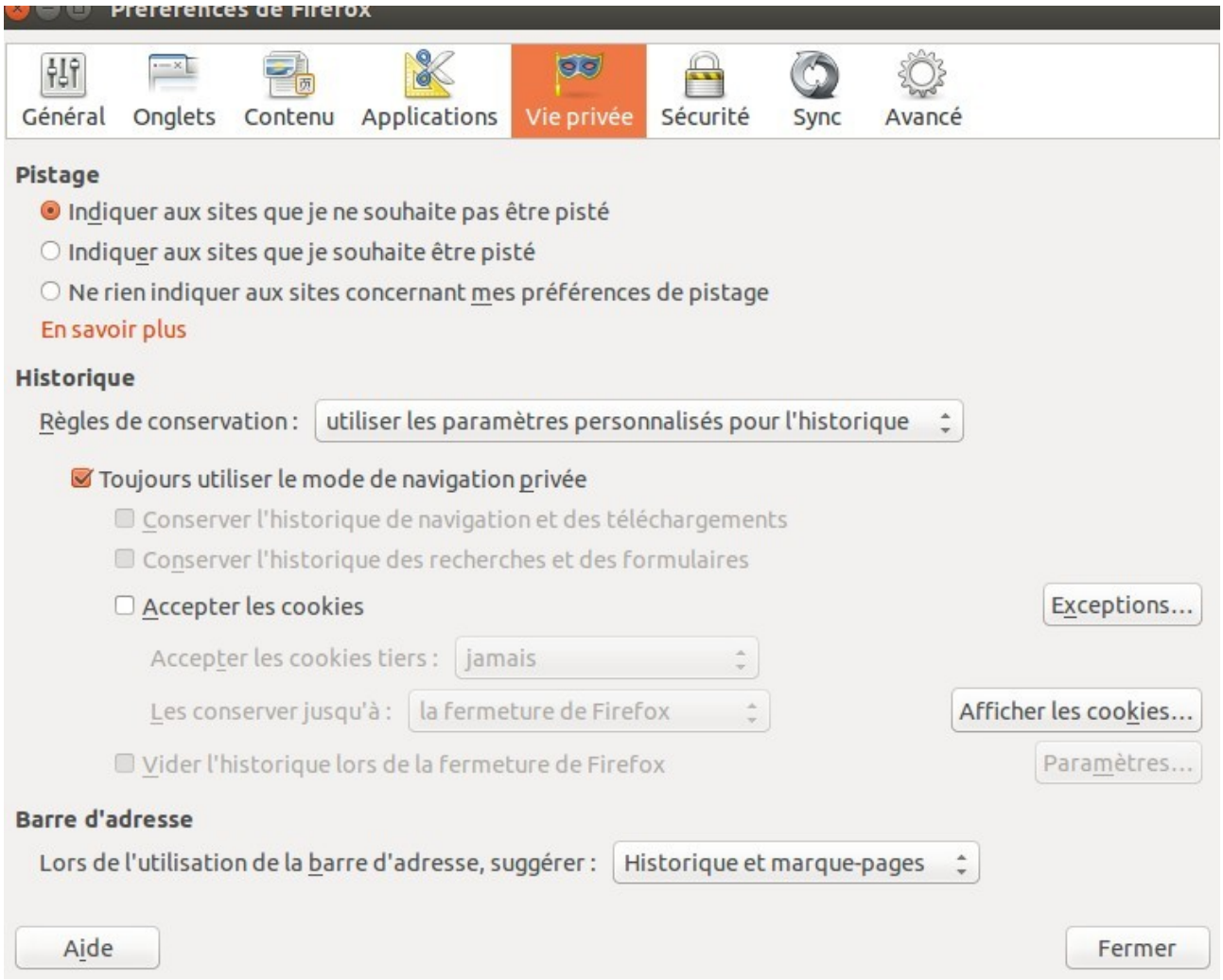
a) Configurer Firefox

Ouvrez Firefox et dans les Préférences allez dans l'onglet « Vie privée »

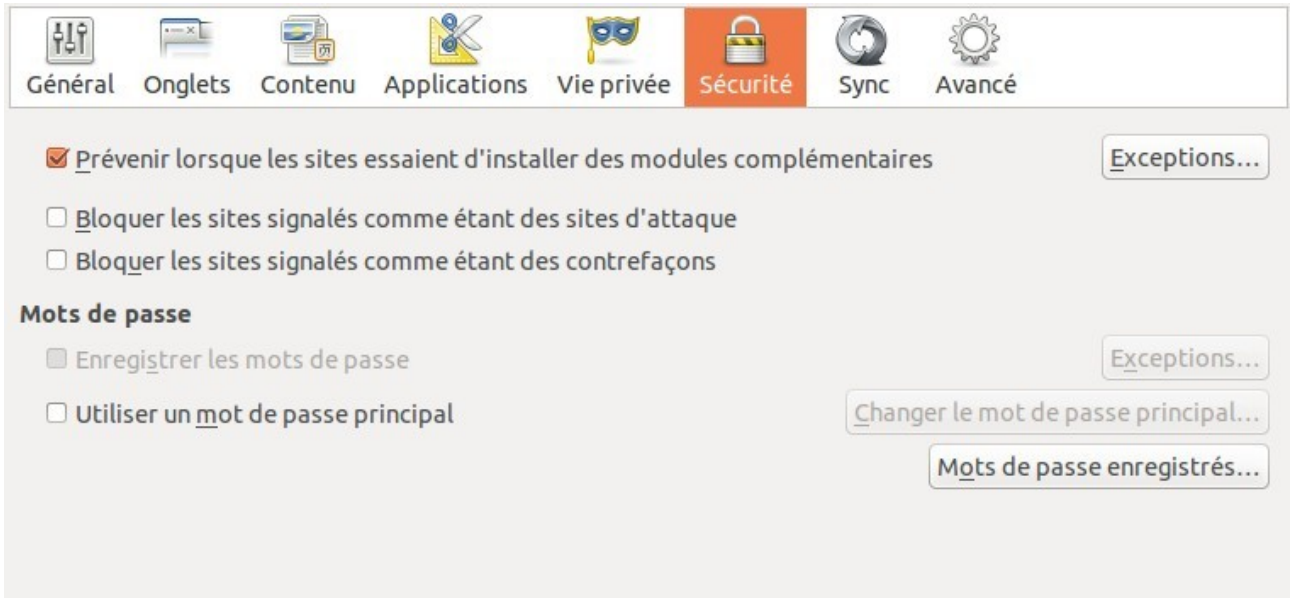
Si vous êtes un utilisateur qui souhaite la facilité au détriment d'une plus grande vie privée, modifiez les paramètres comme sur l'image ci dessous :



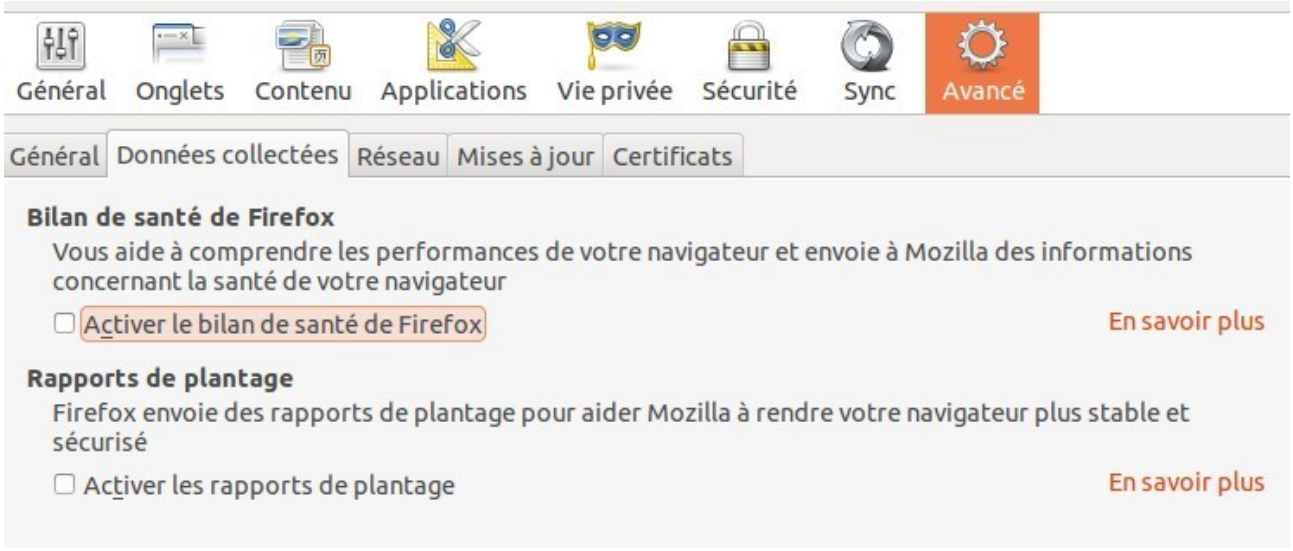
Si par contre vous voulez protéger au maximum votre vie privée, modifiez comme ci-dessous :



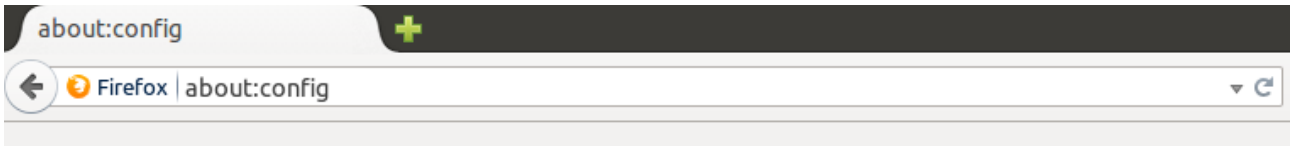
Désactivez la « protection » dans l'onglet sécurité



Désactivez les rapports de plantage et le bilan santé Firefox



Dans la barre d'adresse écrivez « about:config » et faites entrée :



Recherchez et modifiez ces valeurs :

browser.sessionhistory.max_entries -----> 10

browser.bookmarks.max_backups -----> 0 (les marques-pages peuvent révéler des informations très sensibles sur les centres d'intérêts d'une personne)

geo.enabled -----> false (dangereux si vous utilisez un VPN)

browser.display.use_document_fonts ----> 0 (certains textes peuvent mal s'afficher, si vous mettez sur 0 pensez à mettre comme police d'écriture Liberation Sans dans les préférences Firefox)

browser.safebrowsing.enabled ---> false

browser.safebrowsing.malware.enabled ---> false

On peut aussi désactiver le referrer, d'autres réglages mais la plupart des sites ne fonctionneront plus correctement alors on ne les désactive pas (vous pouvez toujours le faire)

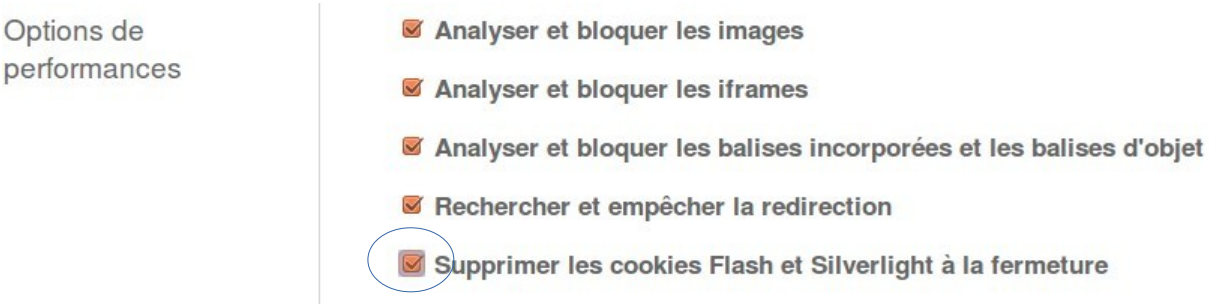
browser.tabs.closeWindowWithLastTab —---> false

browser.preferences.inContent —---> True

b) Installez les modules indispensables :

Adblock : installez le seulement, n'ajoutez pas les filtres pour bloquer les mouchards web (car risque d'incompatibilité avec Ghostery) et désactivez les « publicités acceptables » dans les réglages.

Ghostery: bloquez tous les cookies et les mouchards. Dans les réglages cochez la case pour la suppression des cookies flash



Si par exemple les commentaires sur une page web ne s'affichent pas, activez le service « Disqus » pour la page web (en cliquant sur l'icône Ghostery)

Il y'a aussi d'autres bloqueurs de mouchards comme Disconnect (libre à vous de choisir celui de votre choix)

HTTPS EveryWhere : https://www.eff.org/https-everywhere

Cookie Monster (facultatif) : pour activer ou désactiver les cookies pour un site particulier rapidement en un clic

c) Utiliser des moteurs de recherche qui respectent votre anonymat

Ixquick https://www.ixquick.com	Startpage https://startpage.com	DuckduckGo https://duckduckgo.com
Pensez à régler vos préférences Méta-moteur de recherche qui puise ses résultats dans plus de 100 moteurs sauf Google. Proxy réellement anonyme disponible sous chaque résultat (à utiliser sans modération)	Pensez à régler vos préférences Rechercher sur Google anonymement Proxy réellement anonyme disponible sous chaque résultat (à utiliser sans modération)	Réglez vos préférences si vous voulez des résultats pertinents Très belle interface, rapide et fluide Serveur XMMP gratuit et anonyme (voir la partie communication anonyme du guide)

11] Sécuriser l’exécution de Firefox (obligatoire)

Bravo, vous êtes désormais sous GNU/Linux, vos chances d'être infecté par un virus sont très faibles. Votre système est presque sécurisé, vous utilisez un système d'exploitation libre non-backdooré par la NSA. Vous êtes beaucoup plus en sécurité que sur Windows.

Dans l'immense majorité des cas, les distributions Linux sont équipées avec Firefox comme navigateur web, ce qui fait de Firefox une cible de choix pour tout service de renseignement soucieux d'infecter GNU/Linux (faille 0day dans Tor Browser, etc)

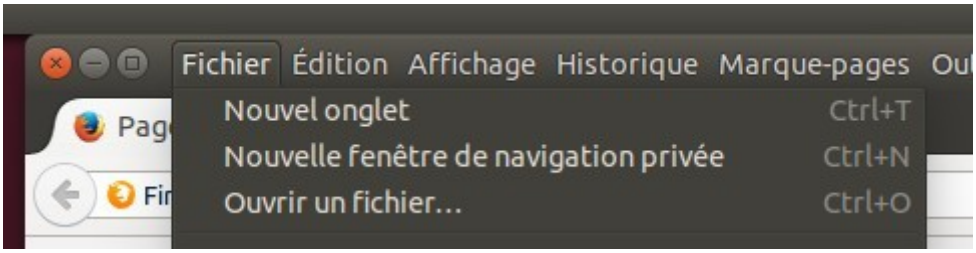
Pour empêcher qu'un exploit 0day ciblant Firefox ne fasse des dégâts considérables, il faut sécuriser Firefox avec le logiciel AppArmor.

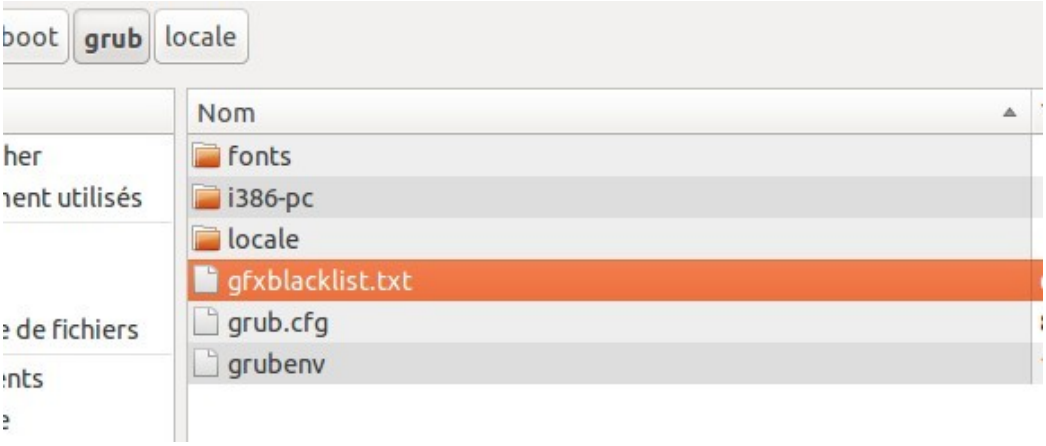
AppArmor est un logiciel libre qui permet de limiter l'exécution et l'accès des programmes au système. https://fr.wikipedia.org/wiki/AppArmor

Par défaut, AppArmor ne protège pas Firefox (incompréhensible), pour le constater faites l'expérience suivante : ouvrez avec Firefox un fichier sensible, par exemple le fichier gfxblacklist.txt

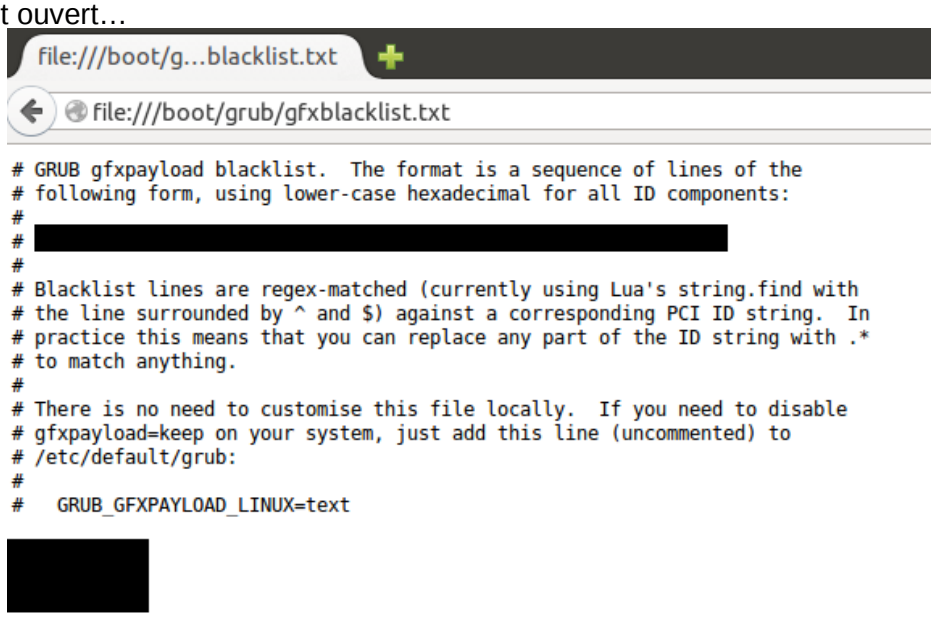
Ce fichier est situé dans la partition /boot, c'est la partition non-chiffrée d'amorçage qui permet le déchiffrement du disque dur lors du démarrage de l'ordinateur. Si Firefox peut y accéder alors un attaquant qui exploite Firefox peut y accéder aussi, il peut modifier la partition /boot et y installer un keylogger qui va enregistrer le mot de passe de chiffrement disque lors du démarrage.

Un attaquant exploitant Firefox peut aussi compromettre le système avec un trojan ou n'importe quel virus made in NSA.





Le fichier est ouvert…



a) Pour protéger le système vous devez sécuriser Firefox avec AppArmor :

Ouvrez un terminal et installez AppArmor :

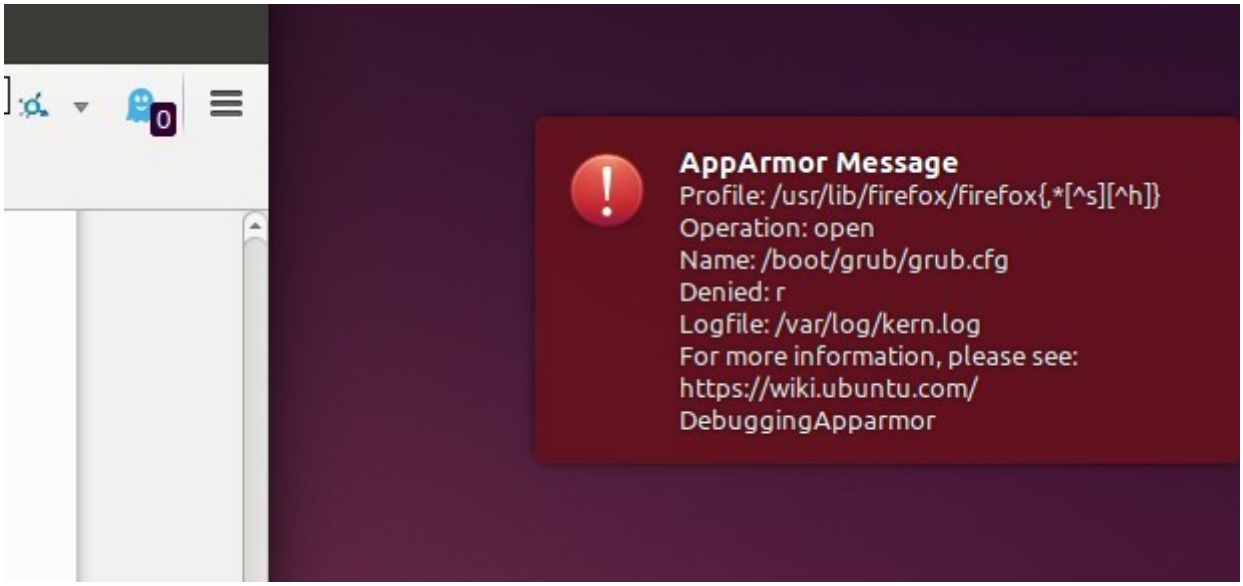
- sudo apt-get install apparmor-utils apparmor-profiles apparmor-notify

Il faut passer le profil de Firefox en mode « enforce »

- sudo aa-status | grep firefox
- sudo aa-enforce /etc/apparmor.d/usr.bin.firefox
- sudo aa-status | grep firefox

Les binaires Firefox sont désormais en mode « enforce »

Vous devez redémarrer pour appliquer les changements. Vérifiez si Firefox est bien en mode « enforce » en essayant à nouveau d'ouvrir un fichier sensible. On obtient une notification indiquant que AppArmor a bloqué Firefox lorsque celui-ci a tenté d'ouvrir un fichier dont il n'a pas les droits d'accès..



b) Pendant que vous y êtes, ajoutez d'autres processus et binaires en mode «enforce » pour diminuer les risques de compromission

https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/AppArmorProfiles

Ouvrez un terminal et vérifiez l'état des profils :

- sudo apparmor_status

```
apparmor module is loaded.
46 profiles are loaded.
22 profiles are in enforce mode.
   /sbin/dhclient
   /usr/bin/evince
   /usr/bin/evince-previewer
   /usr/bin/evince-previewer//sanitized_helper
   /usr/bin/evince-thumbnailer
   /usr/bin/evince-thumbnailer//sanitized_helper
   /usr/bin/evince//sanitized_helper
   /usr/lib/NetworkManager/nm-dhcp-client.action
   /usr/lib/chromium-browser/chromium-browser//browser_java
   /usr/lib/chromium-browser/chromium-browser//browser_openjdk
   /usr/lib/chromium-browser/chromium-browser//sanitized_helper
   /usr/lib/connman/scripts/dhclient-script
   /usr/lib/cups/backend/cups-pdf
   /usr/lib/firefox/firefox{,*[^s][^h]}
   /usr/lib/firefox/firefox{,*[^s][^h]}//browser_java
   /usr/lib/firefox/firefox{,*[^s][^h]}//browser_openjdk
   /usr/lib/firefox/firefox{,*[^s][^h]}//sanitized_helper
   /usr/lib/lightdm/lightdm-guest-session
   /usr/lib/lightdm/lightdm-guest-session//chromium
   /usr/sbin/cups-browsed
   /usr/sbin/cupsd
   /usr/sbin/tcpdump
24 profiles are in complain mode.
   /sbin/klogd
   /sbin/syslog-ng
   /sbin/syslogd
   /usr/lib/chromium-browser/chromium-browser
   /usr/lib/chromium-browser/chromium-browser//chromium_browser_sandbox
   /usr/lib/chromium-browser/chromium-browser//lsb_release
   /usr/lib/chromium-browser/chromium-browser//xdgsettings
   /usr/lib/dovecot/deliver
   /usr/lib/dovecot/dovecot-auth
   /usr/lib/dovecot/imap
   /usr/lib/dovecot/imap-login
   /usr/lib/dovecot/managesieve-login
   /usr/lib/dovecot/pop3
   /usr/lib/dovecot/pop3-login
   /usr/sbin/avahi-daemon
   /usr/sbin/dnsmasq
   /usr/sbin/dovecot
   /usr/sbin/identd
   /usr/sbin/mdnsd
   /usr/sbin/nmbd
   /usr/sbin/nscd
   /usr/sbin/smbd
   /usr/{sbin/traceroute,bin/traceroute.db}
   /{usr/,}bin/ping
7 processes have profiles defined.
4 processes are in enforce mode.
   /sbin/dhclient (958)
   /usr/sbin/cups-browsed (1180)
   /usr/sbin/cupsd (1819)
   /usr/sbin/cupsd (1822)
0 processes are in complain mode.
3 processes are unconfined but have a profile defined.
   /usr/sbin/avahi-daemon (733)
   /usr/sbin/avahi-daemon (735)
   /usr/sbin/dnsmasq (1226)
```

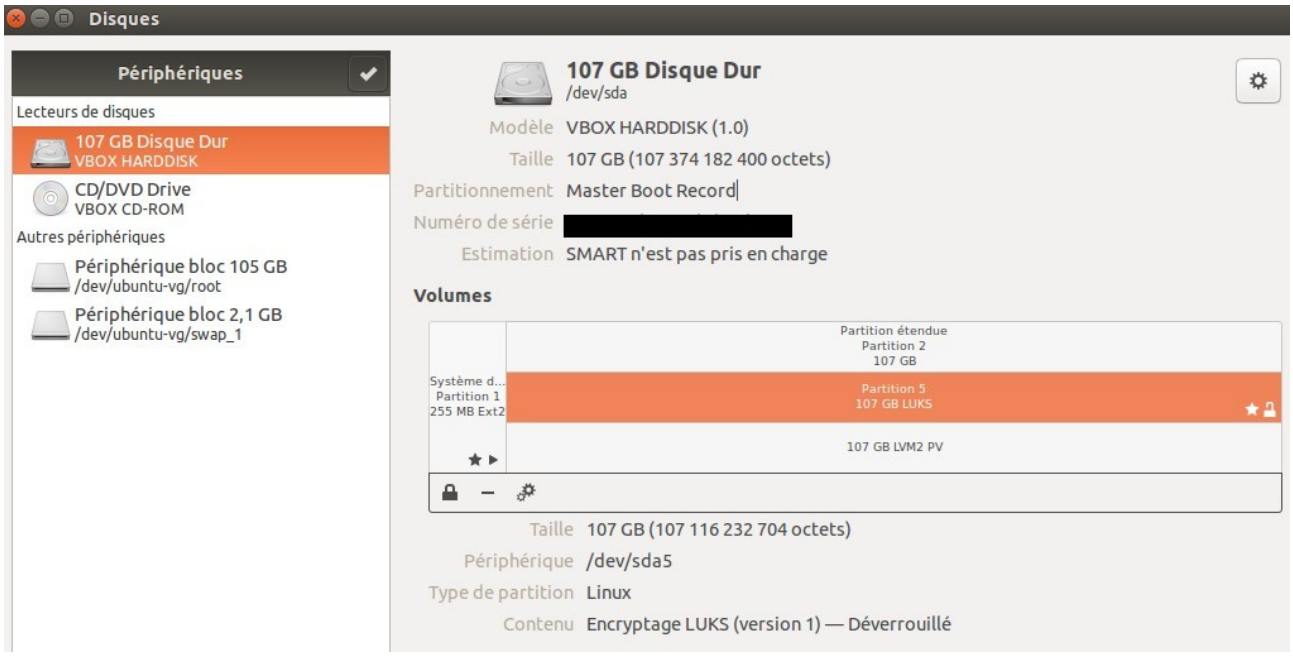
Passez les profils critiques en mode « enforce »

- Les profils d'AppArmor sont localisés dans /etc/apparmor.d
- sudo aa-enforce /etc/apparmor.d/usr.sbin.avahi-daemon
- sudo aa-enforce /etc/apparmor.d/usr.sbin.dnsmasq
- sudo aa-enforce /etc/apparmor.d/usr.sbin.mdnsd
- sudo aa-enforce /etc/apparmor.d/usr.sbin.smbd

Ça devrait suffire. Je n'ai pas testé tous les profils en mode « enforce », donc je ne sais pas si il y'a un impact sur la stabilité mais ceux-là devraient suffire pour une utilisation raisonnablement sûre du système.

12] Vérifier que le disque est bien chiffré (on est jamais trop prudent)

Ouvrez le programme Disque et vérifiez que la partition est bien chiffrée. Le fichier d'échange « swap » doit lui aussi être chiffré (il est lui aussi dans la partition chiffrée)



Faites une vérification plus poussée avec le terminal

- sudo cryptsetup status sda5_crypt

```
/dev/mapper/sda5_crypt is active and is in use.
  type:    LUKS1
  cipher:  aes-xts-plain64
  keysize: 512 bits
  device:  /dev/sda5
  offset:  4096 sectors
  size:    209207296 sectors
  mode:    read/write
  flags:   discards
```

L'installateur d'Ubuntu ne propose pas comme la version alternate la possibilité de modifier les algorithmes de chiffrement. Les devs d'Ubuntu devraient inclure cette option.

L'algorithme est de l'AES-XTS avec une taille de clé de 512bits. C'est un chiffrement très sûr tant que le mot de passe est suffisamment long et complexe.

13] Installer et configurer le par-feu

Via le gestionnaire de paquet synaptic, installez GUFW puis lancez le.

a) Pour les utilisateurs normaux, mettez Incoming sur Refuser et Outgoing sur Autoriser.

C'est largement suffisant pour protéger son système.

Si vous téléchargez via Bittorent n'oubliez pas de désactiver votre par-feu le temps du téléchargement (utilisateurs normaux uniquement)

b) Pour les paranoïaques, mettez tout sur Refuser. Dans ce cas il va falloir spécifier les connexions qui pourront outrepasser le par-feu.

Pour une utilisation normal d'internet, ajoutez les règles suivantes avec le terminal :

- HTTP port 80 : sudo ufw allow out 80
- HTTPS port 443 : sudo ufw allow out 443
- DNS port 53 : sudo ufw allow out 53

Si vous utilisez d'autres programmes (torrent, vpn) soyez sûr que les connexions sont permises pour ce programme.

Si vous n'avez pas envie de vous embêter à rajouter des règles à chaque fois, mettez les règles correspondant aux utilisateurs normaux.

c) Vérifiez souvent les connexions établies ou en cours

- Dans un terminal tapez (merci bziop) : sudo netstat -upan et netstat -tpan

Vérifiez les connexions en cours, soyez sûrs qu'aucune connexion suspecte n'a lieu (normalement il ne doit y avoir aucun problème)

Une IP américaine n'est pas toujours un serveur relais de la NSA en train de pirater votre PC, généralement ce sont les autorités de certifications SSL (qui peuvent aussi êtres compromises par la NSA ou par un MITM, mais c'est un autre sujet)

Si vous n'avez aucune page web ouverte, Firefox est fermé, Bittorent est fermé, aucune connexion n'a lieu et que vous constatez tout de même une IP, alors vous devez vous renseignez sur cette IP.

14] Changer la permission de lecture du dossier /home

Comme vous n'avez pas besoin de partager des fichiers avec des utilisateurs locaux, changez la permission de lecture du dossier /home. Ouvrez un terminal et écrivez :

- sudo chmod 750 /home/VotreNomUtilisateur

15] Désactiver le compte Invité (par mesure de sûreté)

Dans un terminal tapez :

- sudo touch /etc/lightdm/lightdm.conf
- sudo nano /etc/lightdm/lightdm.conf

Ajoutez le texte suivant :
[SeatDefaults]
greeter-show-remote-login=false
allow-guest=false

CTRL + X et sauvegardez,

16] Réduire les droits d'accès aux logs système

Par défaut, les utilisateurs non-privilégiés peuvent accéder aux logs système. Ces logs contiennent des informations critiques pour un attaquant qui espère exploiter votre système.

Dans un terminal copiez-collez :

- sudo bash
- sudo echo kernel.dmesg_restrict = 1 >> /etc/sysctl.conf

17] Réduire les droits d'exécution pour le dossier /tmp

Beaucoup de programmes ont besoin d'un accès lecture/écriture pour le dossier /tmp, mais aucun programme ne devrait avoir les droits d'exécution à partir du dossier /tmp. C'est la raison pour laquelle monter le dossier /tmp avec les options noexec (exécution interdite), nodev, nosuid peut procurer une meilleure sécurité.

Ouvrir un terminal et écrire :

- sudo gedit

Ouvrir avec l'éditeur texte le fichier fstab localisé dans /etc/

NE TOUCHEZ A RIEN et ajoutez à la fin du texte l'argument suivant :

- tmpfs /tmp tmpfs mode=1777,nosuid,nodev,noexec 0 0

Enregistrez puis quittez l'éditeur texte.

Vous devez redémarrer pour appliquer tous les changements.

18] Grsecurity et PaX (utilisateurs très avancés uniquement)

Grsecurity et PaX sont des patchs qui s'appliquent au kernel linux pour littéralement le transformer en bunker. Pour les appliquer il faut recompiler manuellement le kernel linux.

C'est vraiment la manipulation ultime pour les gens extrêmement paranoïaques. La stabilité du système risque d'être affectée, je n'ai pas encore testé les paramètres donc on verra cette partie une autre fois.

19] Faire un audit du système avec Lynis (la touche finale)

Lynis est un logiciel libre qui permet d'auditer complètement son système à la recherche de faille de sécurité.

- Téléchargez la dernière version puis l'extraire : http://rootkit.nl/projects/lynis.html

Se placer avec un terminal dans le dossier d'extraction

- cd lynis-1.5.6

Fermez tous les programmes en cours puis lancez Lynis :

- sudo ./lynis -c -Q

Attendez la fin de l'analyse, il y'a beaucoup de faux positifs, il faut savoir les distinguer par rapport aux vrais menaces.

20] N'installez JAMAIS des programmes provenant d'une source incertaine

N'installez des fichiers deb ou des programmes SI ET SEULEMENT SI vous êtes ABSOLUMENT certain de la fiabilité de la source. Backdoorer un deb est extrêmement facile et si vous installez un deb vérolé S'EN EST FINI de la sécurité de votre système.

SOYEZ ABSOLUMENT CERTAIN DE LA FIABILITE D'UN DEB !!

N'installez jamais un deb que quelqu'un propose comme ça sur le net ou sur un forum, à moins que la personne soit vraiment très fiable et reconnue.

21] Changer transitoirement d'adresse MAC (facultatif)

L'interface réseau est à changer suivant le type d'interface que vous avez
wlan0 → interface Wifi
eth0 → interface Ethernet (câble)

Avec macchanger (pré-installé sous TAILS et Kali Linux)

Ouvrir un terminal et écrire :

- sudo apt-get install macchanger
- sudo ifconfig wlan0 down
- sudo macchanger -a wlan0
- sudo ifconfig wlan0 up

Ensuite vérifier l'attribution de l'adresse MAC avec la commande « ifconfig »

Sans macchanger

Générer une fausse adresse mac valide http://www.miniwebtool.com/mac-address-generator/

Ensuite écrire dans un terminal :

- sudo ifconfig wlan0 down
- sudo ifconfig wlan0 hw ether 01:02:03:04:05:06
- sudo ifconfig wlan0 up

Vérifier l'attribution avec « ifconfig »

22] Changer d'adresse MAC définitivement (facultatif)

Pour changer de façon permanente l'adresse MAC sous Linux, il faut modifier le fichier « interfaces » localisé dans /etc/network/interfaces/

1) Ouvrir un éditeur texte en mode root (gedit par exemple) avec le terminal

- sudo gedit

2) Ouvrir avec l'éditeur texte le fichier « interfaces » localisé dans /etc/network/interfaces/

3) Générer une fausse adresse MAC valide http://www.miniwebtool.com/mac-address-generator/

4) Ajouter à la fin du fichier interfaces l'argument suivant :

pre-up ifconfig wlan0 hw ether 01:02:03:04:05:06

Enregistrer et redémarrer.

23] Protection partielle contre l'attaque de type EVIL MAID (paranoïa)

- Le disque dur est maintenant complètement chiffré, le chiffrement protégera les données si quelqu'un subtilise votre ordinateur et tente d'accéder aux informations contenues dans le disque dur.

- Mais un ennemi suffisamment puissant saura par avance que vos données sont chiffrées, il ne s'embêtera pas à casser le chiffrement par une attaque brute-force, ce serait une perte de temps surtout si votre mot de passe est conforme à la réglementation minimale exigée.

Il va procéder de différente manière pour identifier votre mot de passe

1) Interception électromagnétique

- L'attaquant essayera d'intercepter à distance les ondes électromagnétiques (TEMPEST) émises par votre clavier lorsque vous écrirez le mot de passe de chiffrement lors du démarrage de l'ordinateur.

- C'est la 1ere option qu'un attaquant utilisera pour identifier votre mot de passe. L'attaquant peut même voir à distance en temps réel ce qui est affiché sur votre écran (à cause des ondes de votre écran)

Contre-mesure : seule l'utilisation d'une cage de Faraday est capable de venir à bout de cette attaque. Les spécifications techniques de la cage de Faraday devront être conformes aux normes requises pour empêcher les émanations électromagnétiques de sortir de la cage.

2) L'attaque de type EVIL MAID (compromission physique logicielle)

Si l'interception électromagnétique n'a pas fonctionné, l'attaquant essayera cette option. Ce genre d'ennemi déteste par dessus tout faire prendre conscience à ses cibles qu'elles sont surveillées…

Cette attaque repose sur le fait que le disque n'est pas entièrement chiffré, seule une petite partition d'amorçage, la partition /boot, n'est pas chiffrée. C'est la partition qui permet au système d'exploitation de démarrer l'OS en déchiffrant les données du disque dur.

Scénario classique d'une attaque de type EVIL MAID :

- Vous êtes un ingénieur qualifié qui séjourne dans un hôtel. Le temps d'une pause, vous laissez votre ordinateur chiffré dans votre chambre puis vous partez boire un coup.

- Une femme de ménage (en réalité une technicienne de la NSA, DGSI, MI6 etc) entre dans votre chambre.

- Elle en profite pour insérer une clé usb dans votre ordinateur qui va se charger de modifier la partition /boot d'amorçage (non-chiffrée).

- La partition /boot est en réalité infectée par un simple keylogger (enregistreur de frappe)

- Vous revenez dans votre chambre puis vous démarrez votre ordinateur. Lorsque vous entrez le mot de passe de chiffrement pour déchiffrer l'ordinateur, le keylogger se charge d'enregistrer votre mot de passe.

- Il ne rester plus qu'à subtiliser votre ordinateur lors d'une perquisition par exemple pour avoir accès à votre mot de passe et donc à vos données chiffrées.

Contre-mesure 1	Limite
• Mettre un mot de passe au BIOS empêchant les personnes non autorisées à démarrer le PC sur un liveCD vérolé.	• Le mot de passe BIOS ne fonctionnera pas sur un ordinateur fixe car l'attaquant pourra facilement démonter le disque dur pour le brancher sur son propre matériel. C'est aussi la même chose pour les PC portables avec disque dur démontable. • De plus il pourra même réinitialiser le BIOS en enlevant pendant quelques secondes la pile du BIOS. • Il pourra aussi utiliser une backdoor dans le BIOS pour bypasser le mot de passe BIOS.
Contre-mesure 2	Limite
• Faire une somme de contrôle (hash) de la partition /boot à chaque fermeture et ouverture de l'ordinateur. C'est cette technique que nous allons étudier ici	• Fortement contraignant. • Risque de faux positifs qui suscitent un sentiment de paranoïa persistant mais néanmoins évitable.

Attaque EVIL MAID : contre-mesure 2 (hash de la partition /boot)

1) Installer Kali Linux sur une clé usb http://www.kali.org/downloads/

2) Démarrer sur Kali Linux en MODE FORENSICS

3) Localiser avec le programme Disk Utility le chemin de la partition /boot SANS JAMAIS LE MONTER OU LE TOUCHER.

4) Normalement le chemin de la partition /boot est du genre /dev/sdaX (ex : /dev/sda2)

5) Générer un hash SHA512 de la partition /boot avec le terminal :
- sha512sum /dev/sdaX

6) Planquer la somme de contrôle dans un volume TrueCrypt (un hidden volume est souhaitable) situé dans la clé usb qui contient le système Kali Linux (pour plus de facilité)
- Kali Linux contient déjà TrueCrypt pré-installé.

7) Éteindre le PC sans toucher ou monter la partition /boot

8) Conserver cette clé usb dans un endroit extrêmement sécurisé.

Vous possédez donc le hash de la partition /boot à un instant donné.

Si pendant votre absence quelqu'un s'amuse à modifier ne serait-ce qu'un octet de la partition /boot, la somme de contrôle sera DIFFERENTE, vous pourrez ainsi détecter une attaque de type EVIL MAID et agir en conséquence.

Attention aux faux positifs :

- Il suffit de démarrer le PC pour que le BIOS charge la partition /boot (afin que vous écriviez le mot de passe permettant de déchiffrer le disque dur), et bien rien que cette action MODIFIERA la somme de contrôle vous faisant ainsi penser à tort que quelqu'un a modifié votre partition /boot…

- Donc ne permettez à personne ne serait-ce de démarrer le PC, parce que ceci chargera la partition /boot et modifiera sa somme de contrôle.

- Même démarrer avec un liveCD Ubuntu peut modifier le hash de la partition /boot. Seul Kali Linux en MODE FORENSICS ne modifiera pas le hash.

- D'où l'intérêt de mettre un mot de passe BIOS qui empêchera au moins le chargement de la partition /boot si il y'a un démarrage involontaire de l'ordinateur.

Vérifiez la somme de contrôle de la partition /boot à CHAQUE démarrage

- Suivez la même procédure que dans la page précédente.

En cas de détection AVÉRÉE d'une tentative d'attaque EVIL MAID

- Vous vous êtes absentés en laissant votre PC sans surveillance pendant un temps déterminé (jours, semaines, heures...)
- Vous avez vérifié la somme de contrôle de la partition /boot avant de démarrer le PC et elle est différente…
- Vous êtes pourtant absolument certain de ne pas avoir démarrer le PC avant par erreur, d'avoir modifier ou toucher la partition /boot (avec un quelconque livecd linux)
- Vous êtes sûrs qu'aucune personne de votre entourage ne s'est amusé à trifouiller votre PC.

Dans ce cas quelqu'un a modifié la partition /boot avec un keylogger pour identifier votre mot de passe.

1) Démarrez le PC avec Kali Linux
2) Déchiffrez votre disque dur DANS le liveCD ou alors faites une copie de votre partition chiffrée pour l'ouvrir dans un environnement plus sécurisé.

3) Compromission physique matérielle

- Au lieu d'installer un keylogger logiciel, l'attaquant installe ce coup-ci un keylogger matériel (dans votre clavier, sur la carte mère)

- Aucune technique logicielle n'est capable de détecter cette attaque. Seule une vérification visuelle des composants internes de l'ordinateur permet de déceler le composant nuisible.

- Cette attaque est plus difficile sur les ordinateurs portables (je n'ai trouvé aucune information faisant état d'une telle attaque sur un PC portable…) mais elle n'est certainement pas impossible.

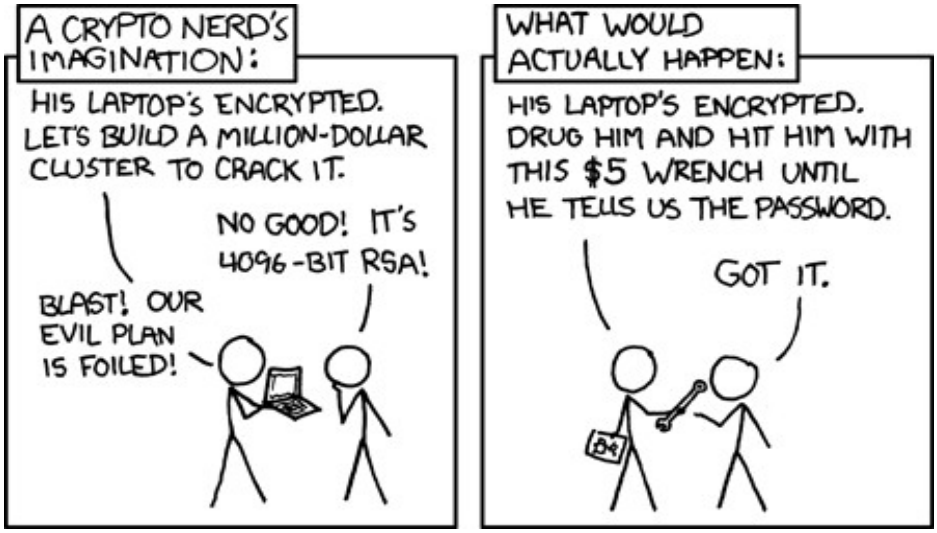
- Cette attaque est très facilement réalisable sur un ordinateur fixe.

- Des services de renseignements extrêmement sophistiqués comme la NSA peuvent même remplacer le CPU par un CPU identique mais compromis…. Aucune technique n'existe pour détecter ce genre d'attaque.

- C'est l'attaque ultime, personne ne peut s'en prémunir, il faut veiller à la sécurité physique de son ordinateur et acheter ses composants directement en liquide depuis un magasin « sûr ».

- Seules des cibles de très haute priorités sont susceptibles d'être visées par une telle attaque. Et dans ce type de contexte, mieux vaut ne pas utiliser le moindre matériel informatique.

4) La coercition physique (tabassage, torture, intimidation)



Contre-mesure 1	Limite
• Être totalement anonyme. Si l'ennemi ne sait pas qui vous êtes, il ne peut vous faire du mal.	• Commettre la moindre erreur entraînant une dé-anonymisation vous condamnera à ne plus jamais être en sécurité sur Terre. • Techniquement fastidieux et compliqué. • Risque d'erreur.
Contre-mesure 2	Limite
• Être armé et prêt à se défendre physiquement (gilet par-balle, etc)	• Risque de mort lors d'un affrontement avec une équipe des forces spéciales.
Contre-mesure 3	Limite
• Fuir le pays.	• Nécessite une préparation technique et financière. • Difficile dans les pays à tendance totalitaire (USA, France)

LOGICIELS INDISPENSABLES

MAT: anonymiser les photos et documents (suppression EXIF)

Installez le via le gestionnaire synaptic (Metadata Anonymisation Toolkit)

C'est un petit programme très important qui permet de supprimer les données sensibles des fichiers comme les photos (exifs), pdf...

HardInfo : donne les spécifications système avancées (très utile)

Via le gestionnaire Synaptic

Gdebi : installateur de paquet .deb (très utile)

Via le gestionnaire synaptic
Automatise l'installation des paquets .deb

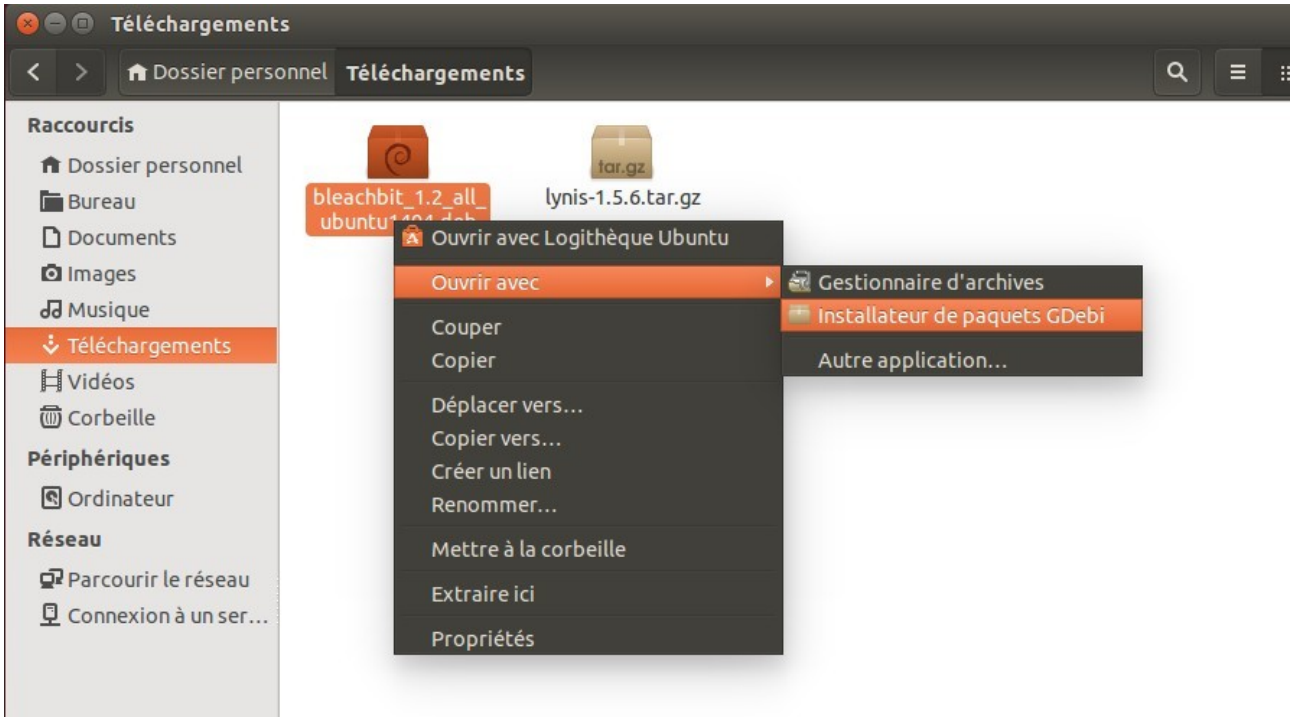
Bleachbit : le couteau suisse pour supprimer l'historique et les traces

Logiciel indispensable pour nettoyer son système des logs d'activité (fichiers ouverts, miniatures des images, traces d'historiques, etc)

Téléchargez la dernière version sur le site officiel (car celle du dépôt ubuntu n'est pas à jour)

http://bleachbit.sourceforge.net/download/linux

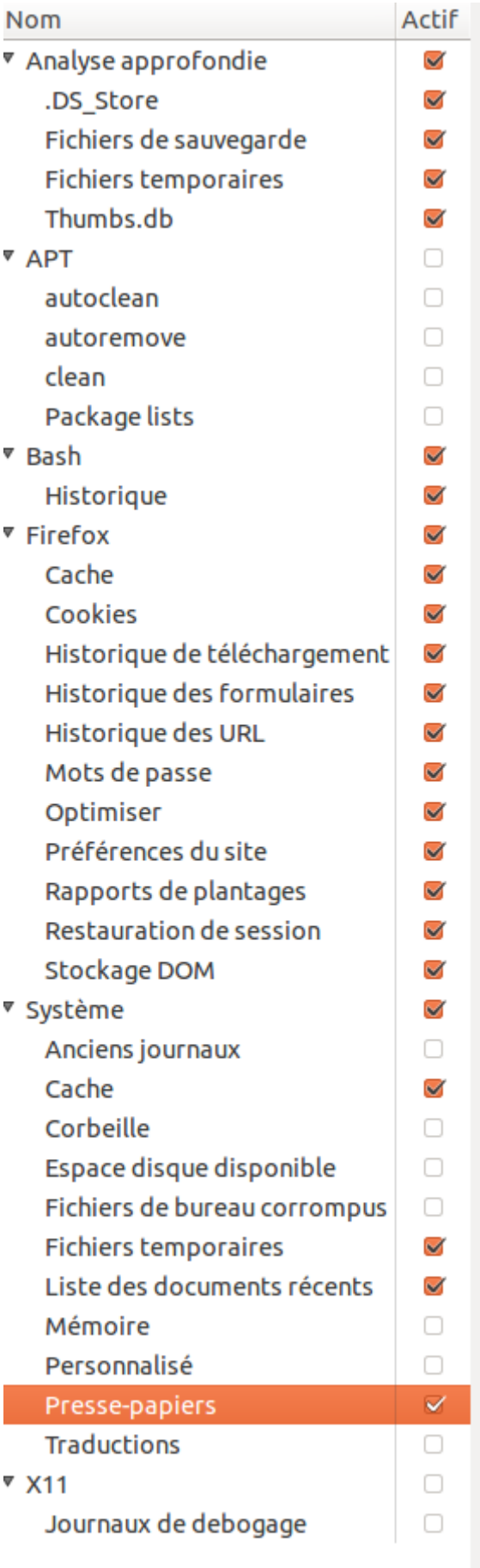
Faites clique-droit et ouvrez le fichier deb avec l'installateur Gdebi



Ensuite installez Bleachbit et lancez-le

Choisissez les paramètres comme sur l'image. Ce sont les paramètres qui permettent de ne pas déstabiliser le système. Testés et approuvés.

Si vous avez installé d'autres logiciel (flashplayer, VLC) vous pouvez aussi en supprimer les traces.



TrueCrypt : pas la peine de le présenter

La version 7.1a de TrueCrypt est SÛRE. Il suffit de rester sur cette version et d'attendre que la communauté prenne le relais et continue le travail.

Veillez cependant à télécharger votre exécutable d'une source sûre : https://truecrypt.ch/

Fichier	Whirlpool (somme de contrôle)
truecrypt-7.1a-linux-x64.tar.gz	e8921d2dcc3ed1f259e528c4ae69ed2863817008940d4924b7aa6e31722dd581e4d5ef38ee8a46741efe1feeaa168ec1cf4a5fd910bb232bfc623d2c7d41db54
truecrypt-7.1a-linux-x86.tar.gz	557f9f02e5258e9f2750f875f5825f5ad78e6fd671b31bb55ae4fe2af12f8d53d7a010fb5de34b71ebc10498fa28b807bb9004280612c5487658118e193ebf47

Comme ce guide s'adresse plus spécifiquement au débutant, voici la méthode pour installer TrueCrypt (les utilisateurs avancées peuvent passer) :

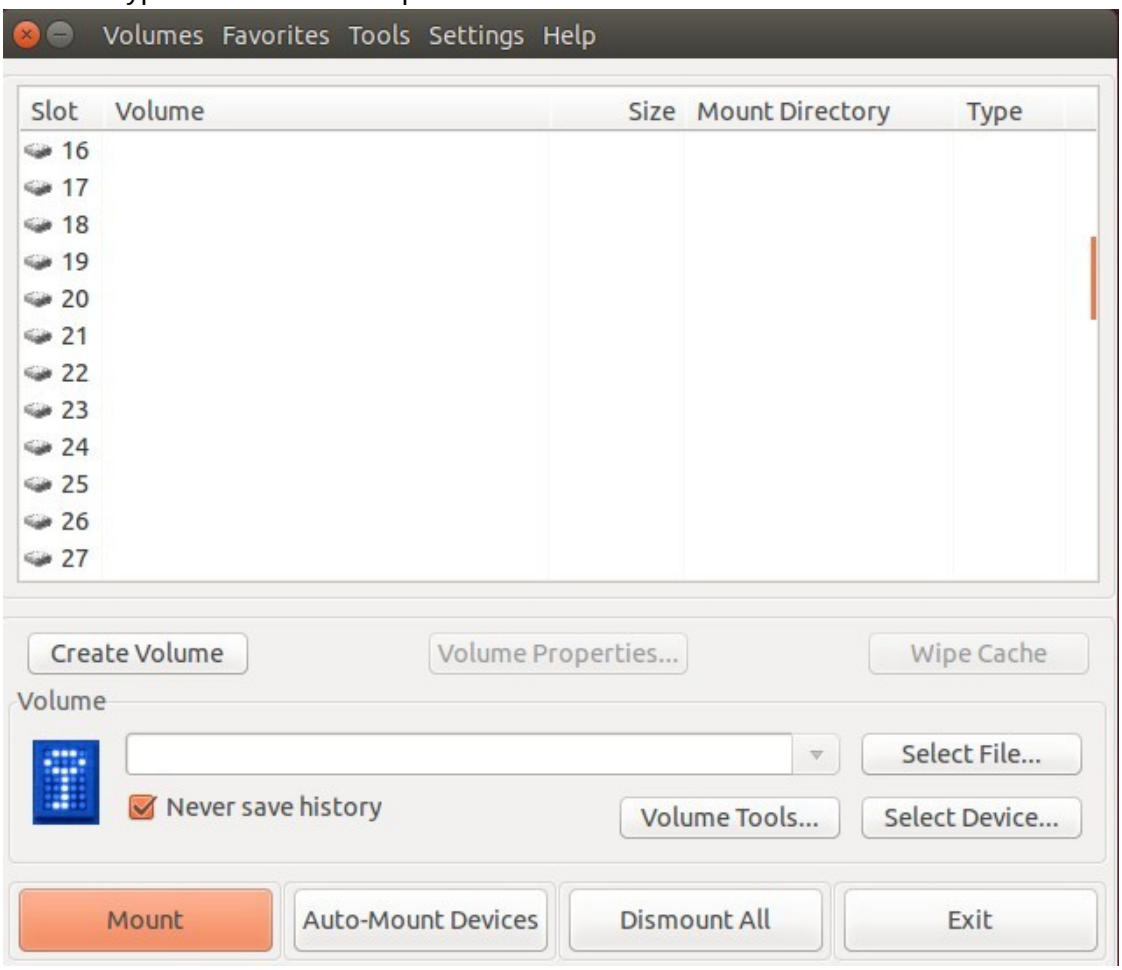
Ouvrez un terminal et placez vous dans le dossier contenant l'exécutable TrueCrypt

- cd Téléchargements

Lancez l'exécutable

./truecrypt-7.1a-setup-x64

Et installez TrueCrypt en suivant les étapes.



VLC Media Player : pas la peine de le présenter

Via gestionnaire synaptic

Lit pratiquement tous les formats multimédia existant.

GtkHash : vérifier la somme de contrôle d'un fichier (hash)

Via gestionnaire synaptic

Petit programme indispensable pour vérifier le hash d'un fichier. Il supporte énormément de hash différent. Très bon logiciel.

GPA: interface graphique pour GNUPG (chiffrement asymétrique)

Via gestionnaire synaptic

Cette interface graphique pour GNUPG est la meilleure disponible sous Ubuntu. Il y'a juste un petit problème qui se produit lors du lancement du logiciel, il faut le corriger :

Après avoir installer GPA allez dans un terminal et tapez :

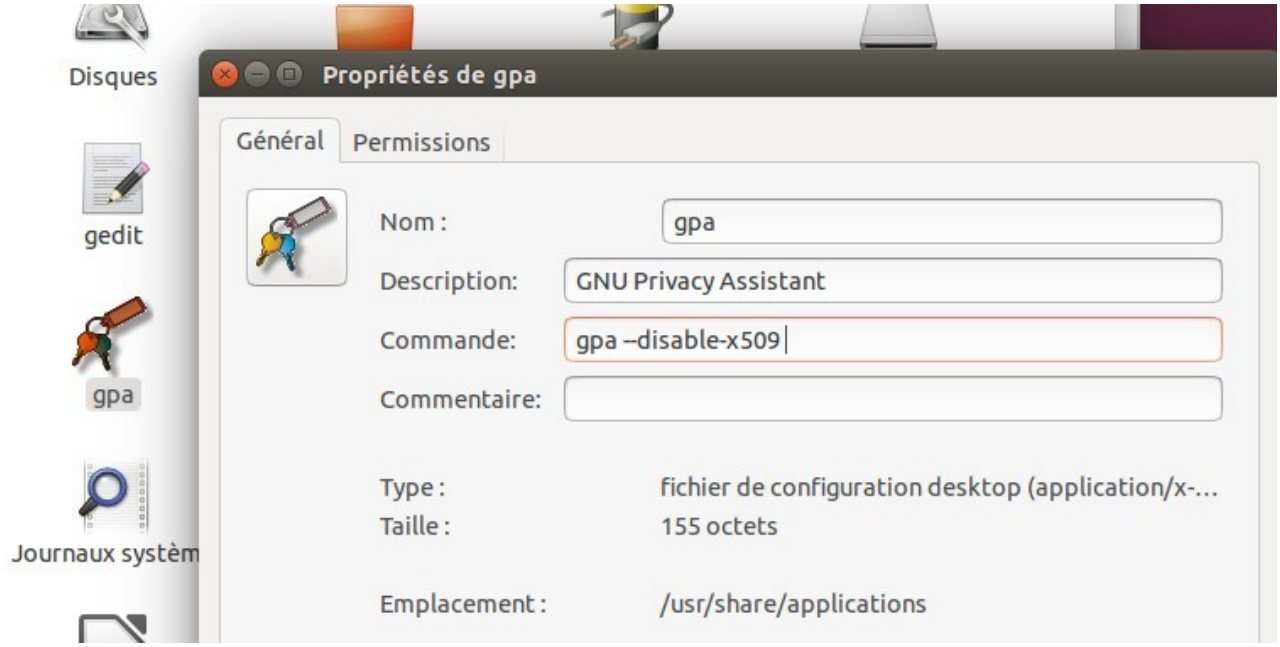
- sudo nautilus

Le gestionnaire de fichier s'ouvre. Allez dans le dossier /usr/share/applications

Recherchez le programme GPA et faites clique-droit dessus ---> Propriétés

Ajoutez dans la ligne « commande » cet argument :

- --disable-x509



Fermez Nautilus puis fermez le terminal. GPA est désormais pleinement fonctionnel.

Ouvrez GPA, allez dans l'onglet « Editer » ---> « Préférences backends »

- Mettez la valeur de « keyserver » sur « Ne pas utiliser l'option »

Vous pouvez par erreur uploader votre clé publique sur un serveur de clé, or cet upload peut se faire avec votre véritable adresse IP, si votre clé publique est connue de tous et que vous l'avez uploadé avec votre propre IP sans faire exprès, votre adresse IP est corrélée à cette clé publique. Vous êtes déanonymisés.

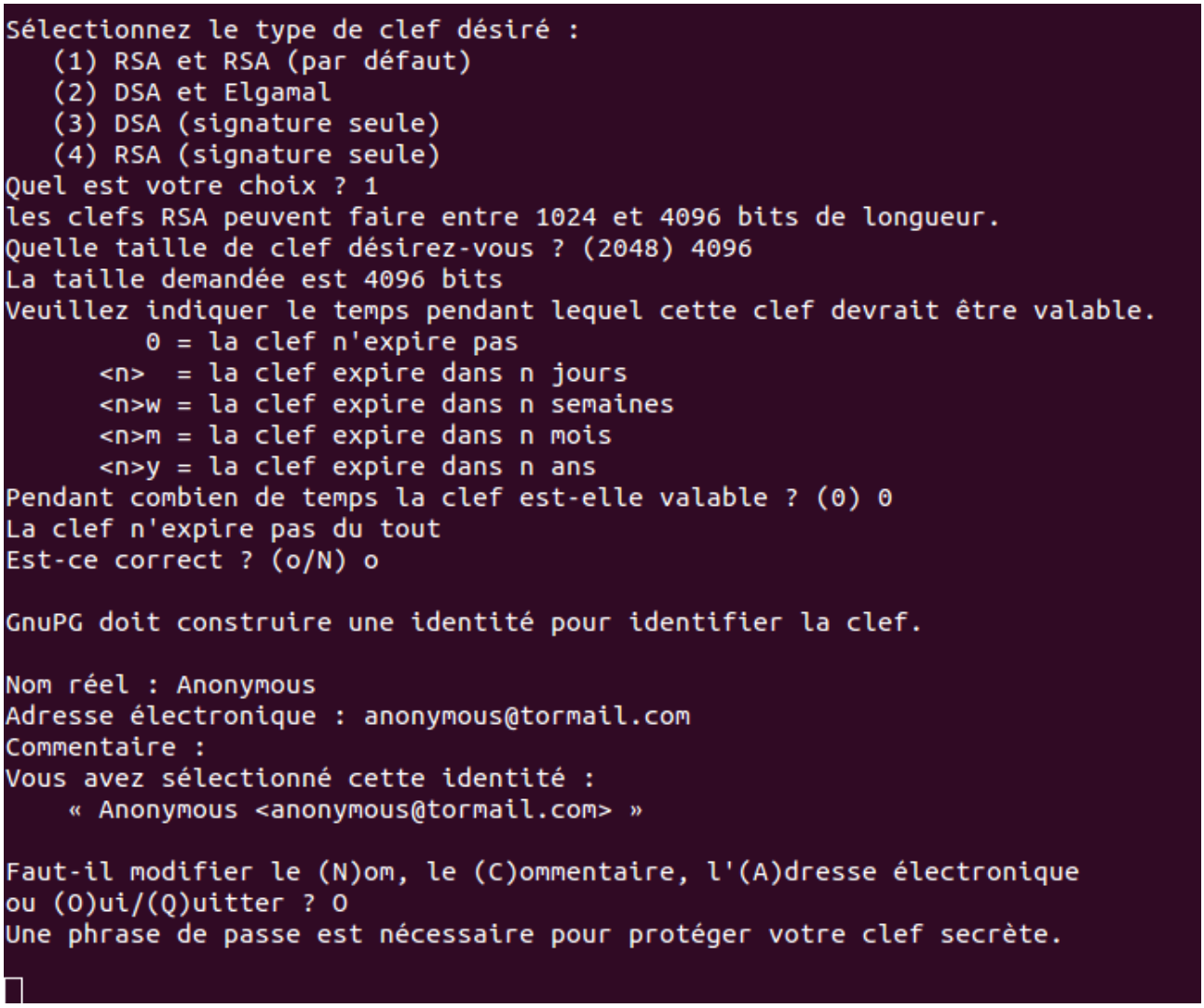
Donc faites très attention en utilisant GPA de ne pas upload involontairement votre clé publique.

Générer sa paire de clé privée/publique (facultatif)

Ouvrir un terminal et écrire :

- gpg2 –gen-key

Suivez les instructions : vous pouvez choisir un délais d'expiration si vous le souhaitez. Mettez des faux nom bien sûr et si possible un email anonyme.



Entrez un mot de passe de minimum 20 caractères (maj, min, chiffre, spéciaux). Vous vous demandez sans doute : comment se fait-il que je peux importer ma clé privée sans que GPA me demande le mot de passe ? Ma clé privée est elle stockée en clair ?

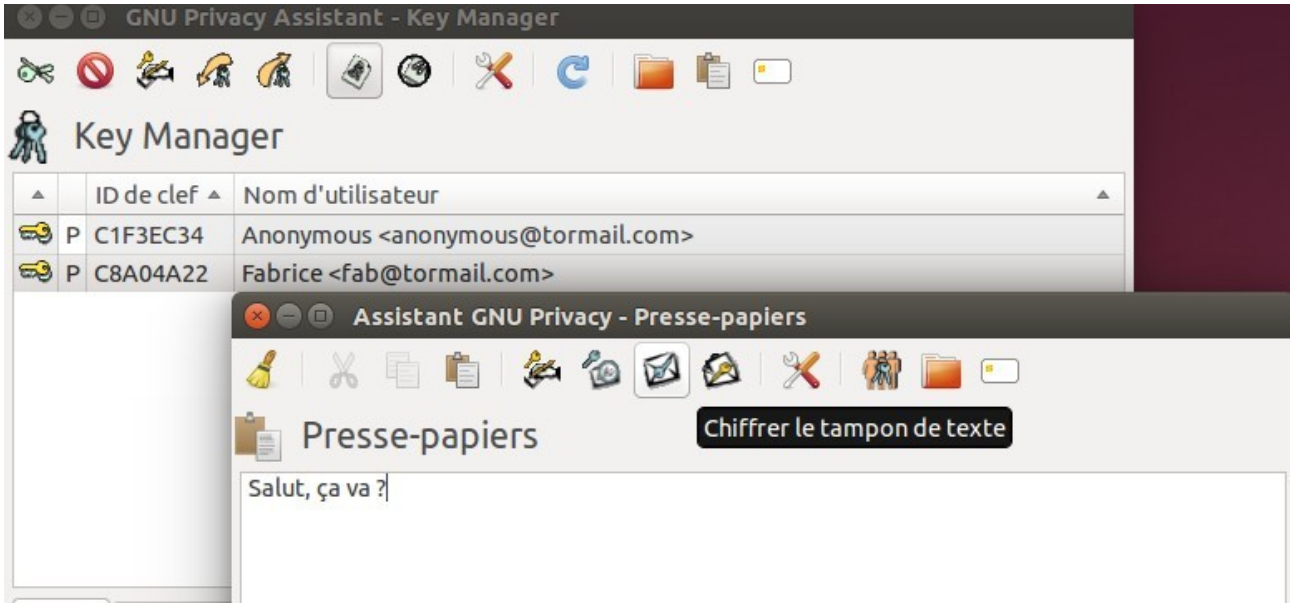
Bien sûr que non, elle est chiffrée avec votre mot de passe en combinaison avec un algorithme de chiffrement

- Générez de l'entropie (déplacer de gros fichier, etc) pour que la clé puisse se créer.
- Une fois votre paire de clé crée, vous devez ajouter la clé publique de votre contact.
- Par exemple sur FDW vous avez un topic où chacun poste ses clé publiques. Copiez-collez la clé de votre contact. Collez sa clé dans un fichier texte et enregistrez le fichier texte.
- Ensuite importez ce fichier texte avec GPA. La clé publique du contact est importée.

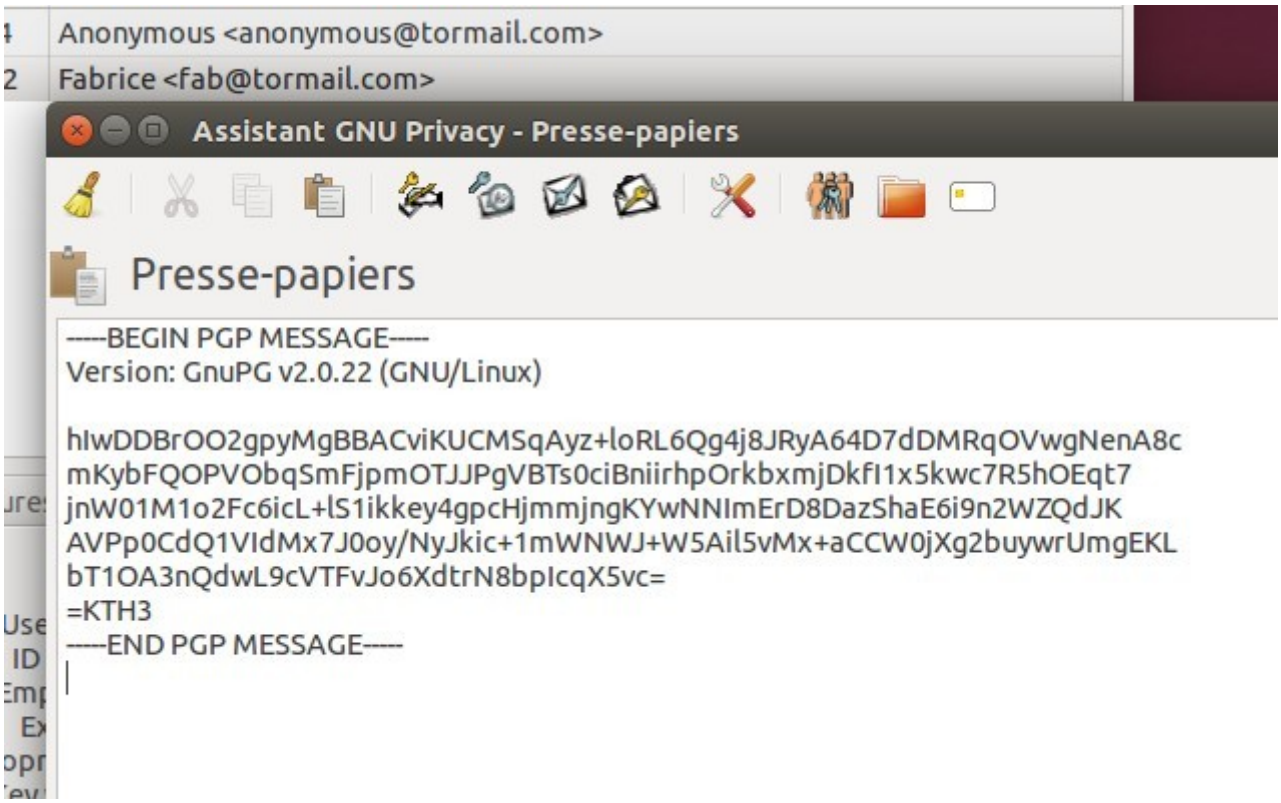
Envoyez un message chiffré à votre contact

Seul votre contact qui est en possession de la clé privée sera en mesure de lire le message chiffré avec sa clé publique que vous lui envoyez.

- Ouvrir le presse-papier dans GPA
- Écrire votre message
- Chiffrer le tampon texte



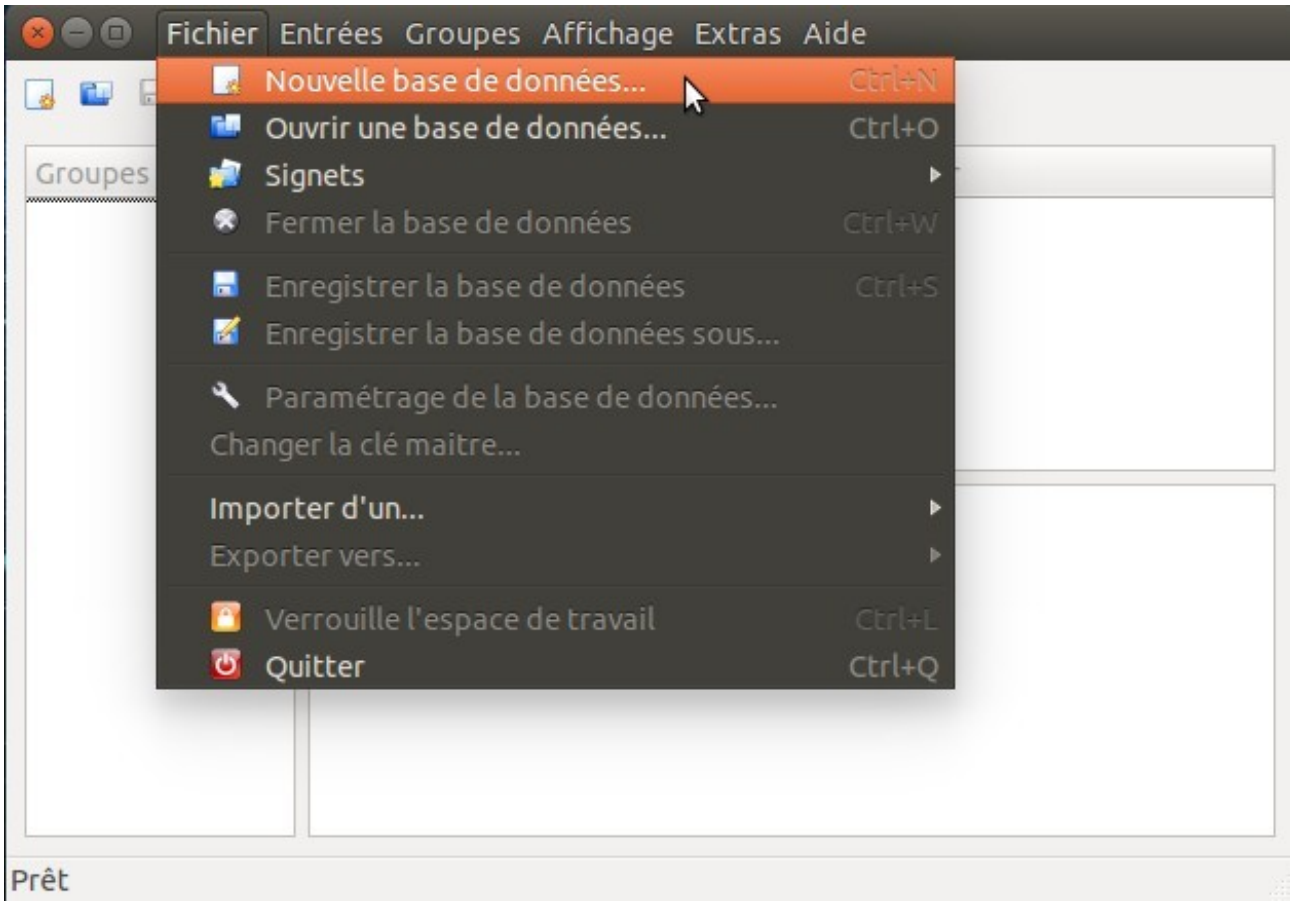
- Choisir la clé publique du contact et chiffrez



Le message est chiffré. Vous pouvez l'envoyer. Déchiffrer un message qui vous est destiné se déroule de la même façon (Déchiffrer le tampon texte)

KeePassx : gestionnaire de mot de passe chiffré

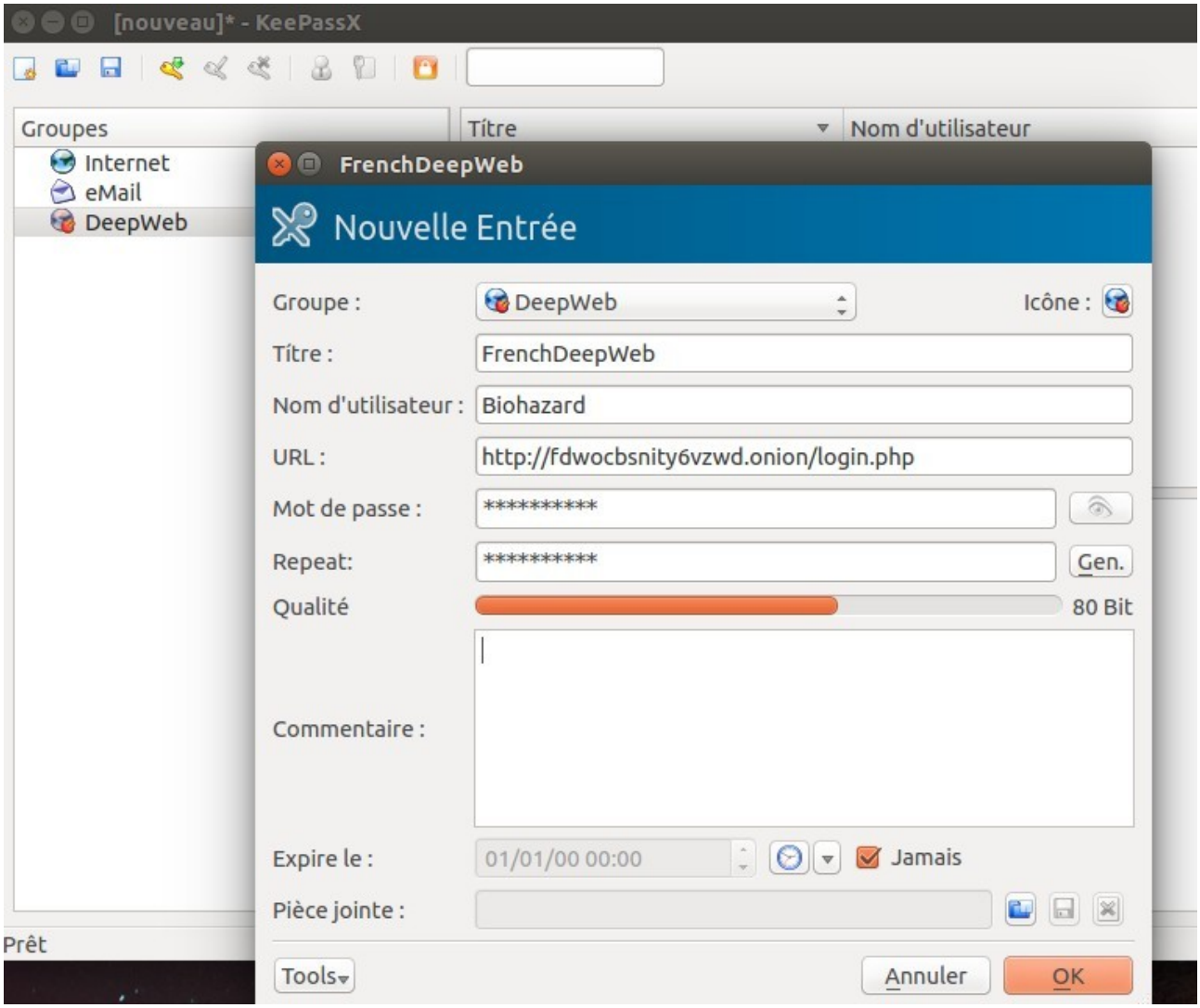
- Installez le paquet « keepassx » via le gestionnaire synaptic
- Lancez KeePassX et créez une nouvelle base de données
- Choisissez un mot de passe long et complexe (ce mot de passe ne doit pas être le même que celui qui sert à chiffrer le disque dur)



- Allez dans Fichier ---> Paramétrage de la base de données, puis cliquez sur l'icône en forme de réveil
- Cela va augmenter dramatiquement le nombre de passes du chiffrement, rendant votre base de donnée beaucoup plus sécurisée.

Ensuite vous pouvez ajouter vos comptes en créant des groupes et des sous-groupes.

N'oubliez pas de sauvegarder votre base de donnée, et faites en des copies !



Vous pouvez utiliser votre base de données dans Android

- Téléchargez l'application KeePassDroid via la logithèque F-Droid.
- Placez votre base donnée sur la carte sd de votre téléphone et ouvrez la avec KeePassDroid.

(voir le tuto de sécurisation d'Android)

GIMP: le photoshop libre

Via gestionnaire synaptic
Très bon logiciel, rapide et complet.

VirtualBox : création de machine virtuelle (très pratique).

Via gestionnaire synaptic

Logiciel très impressionnant qui permet de s'amuser avec les machines virtuelles. Installez windows ou n'importe quel système d'exploitation dans une machine virtuelle, foutez le bordel en toute impunité.

Idéal pour s'entraîner.

Ricochet : communication ultra-sécurisée (comme Torchat)

Des membres du forum ont émis des avertissements sur Torchat car il utilise une ancienne version de TOR et des packages assez anciens, ce qui le rend dangereux à utiliser (ancienne version d'OpenSSL, etc)

Voici une alternative qui fait exactement la même chose que Torchat mais en utilisant des binaires et des packages à jour : https://github.com/ricochet-im/ricochet

Pour télécharger le programme (disponible sous Linux, Windows, Mac)

- https://github.com/ricochet-im/ricochet/releases

Les principales caractéristiques (comme Torchat, rien de bien nouveau)

- Votre adresse IP n'est jamais connue de votre interlocuteur
- Même si votre connexion est sous haute surveillance, personne ne peut identifier avec qui vous parlez, ni encore moins de quoi vous parlez (sauf en cas de compromission du système hôte ou bien d'une interception électromagnétique TEMPEST)
- Rien ne sort de l'espace des hiddens services TOR, pas de nœud de sortie, pas de serveurs centralisés, la NSA ne peut faire pression sur aucun prestataire réseau.

Extrayiez l'archive. Il suffit de l’exécuter, c'est un logiciel portable.

Beaucoup d'autres programmes existent :

- Besoin de faire du traitement de texte ? LibreOffice.
- Besoin d'analyser les paquets qui transitent par votre connexion ? Wireshark
- on va pas tous les faire…

4K Video Downloader (bonus)

Logiciel open-source impressionnant qui est le seul permettant de télécharger avec une facilité déconcertante les vidéos Youtube 4K ou 1080p.

Les autres logiciels ou plugins capable de télécharger les vidéos Youtube en 1080p sont rares et ne fonctionnent pas toujours, de plus pour l'instant j'en ai vu aucun qui soit capable de télécharger du 4K aussi facilement que celui-là !

Les sites supportés sont :

YouTube	Facebook	Vimeo	SoundCloud	Flickr	Dailymotion	Metacafe

Téléchargez le programme

- Même pas la peine de l'installer, prenez une version portable
  http://www.4kdownload.com/fr/download

- Extraire l'archive

Le logiciel ne se lance pas avec l'exécutable parce qu'il tente d'utiliser une autre version de libavcodec.so, c'est embêtant mais pas trop grave.

Inutile de perdre du temps en changeant l'argument libavcodec avec un éditeur hexadécimal.

Ouvrez un terminal et placez vous dans le dossier d'extraction, puis écrivez :

- ./4kvideodownloader.sh

Le logiciel possède d'autres fonctionnalités (mp3, sous-titre, etc)
- http://www.4kdownload.com/fr/products/product-videodownloader
- Possibilité de télécharger les vidéos Youtube interdites -18 sans posséder de compte !! lol

Il y'a des pubs en bas qui n'entravent en rien l'utilisation et le confort du programme.

Respecte votre anonymat, ce que vous téléchargez n'est pas enregistré ni envoyé.
- http://www.4kdownload.com/fr/privacy

Si vous souhaitez l'utiliser sans devoir ouvrir le terminal à chaque fois, installez-le paquet deb avec le logiciel Gdebi.

Bon téléchargement =)

UBUNTU SEUL (MODE UEFI)

Si votre PC est récent, il est équipé du nouveau bios UEFI. Vous devez suivre cette partie pour installer convenablement Ubuntu en mode UEFI.

1] Désactiver les options du bios qui empêchent le boot d'Ubuntu

Plus d'information : http://doc.ubuntu-fr.org/uefi

Lors du démarrage de l'ordinateur, vous devez booter sur le menu du bios

- La façon de faire dépend du modèle du bios, vous devez appuyez sur Echap, F12 ou F10 lors du démarrage.

Désactivez les options suivantes dans le menu du bios :

- QuickBoot (parfois appelé FastBoot)
- Intel Smart Response Technology (SRT)
- Fast Startup
- Secure Boot
- Il vaut mieux passer l'option « OS Type » (si présente) en : Other OS

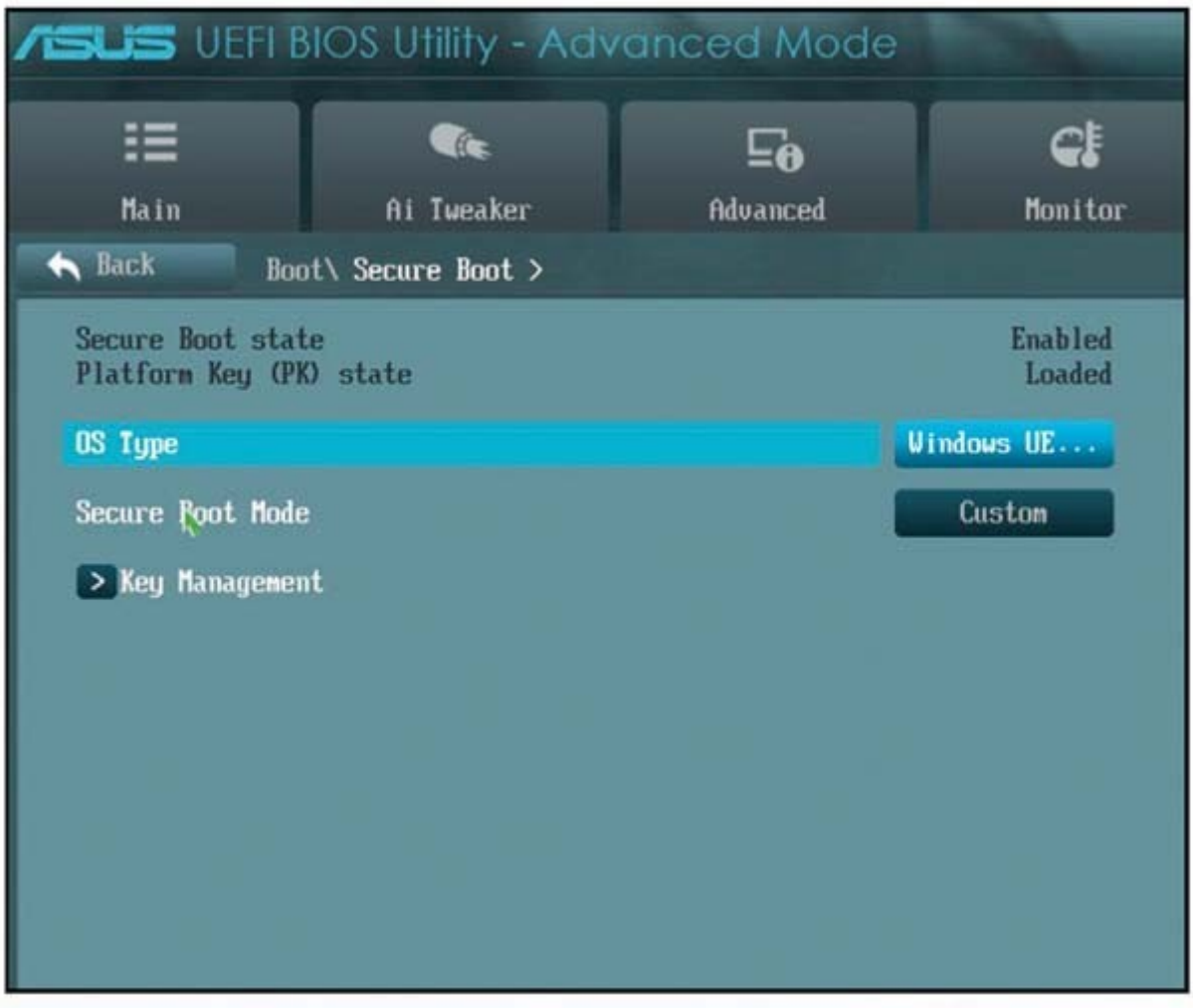
Si certaines options ne sont pas présentes dans le bios, ce n'est pas grave.

Parfois il faut passer le Boot Mode en UEFI

- Il est préférable de régler le paramètre sur « UEFI & Legacy ».
- Le bios vous laissera alors le choix entre un boot normal (legacy) ou UEFI (voir l'image de la page suivante)

Sauvegardez les changements et quittez le bios.

EXEMPLE:



2] Convertir le disque dur en GUID Partition Table (GPT)

Plus d'infos : https://fr.wikipedia.org/wiki/GUID_Partition_Table

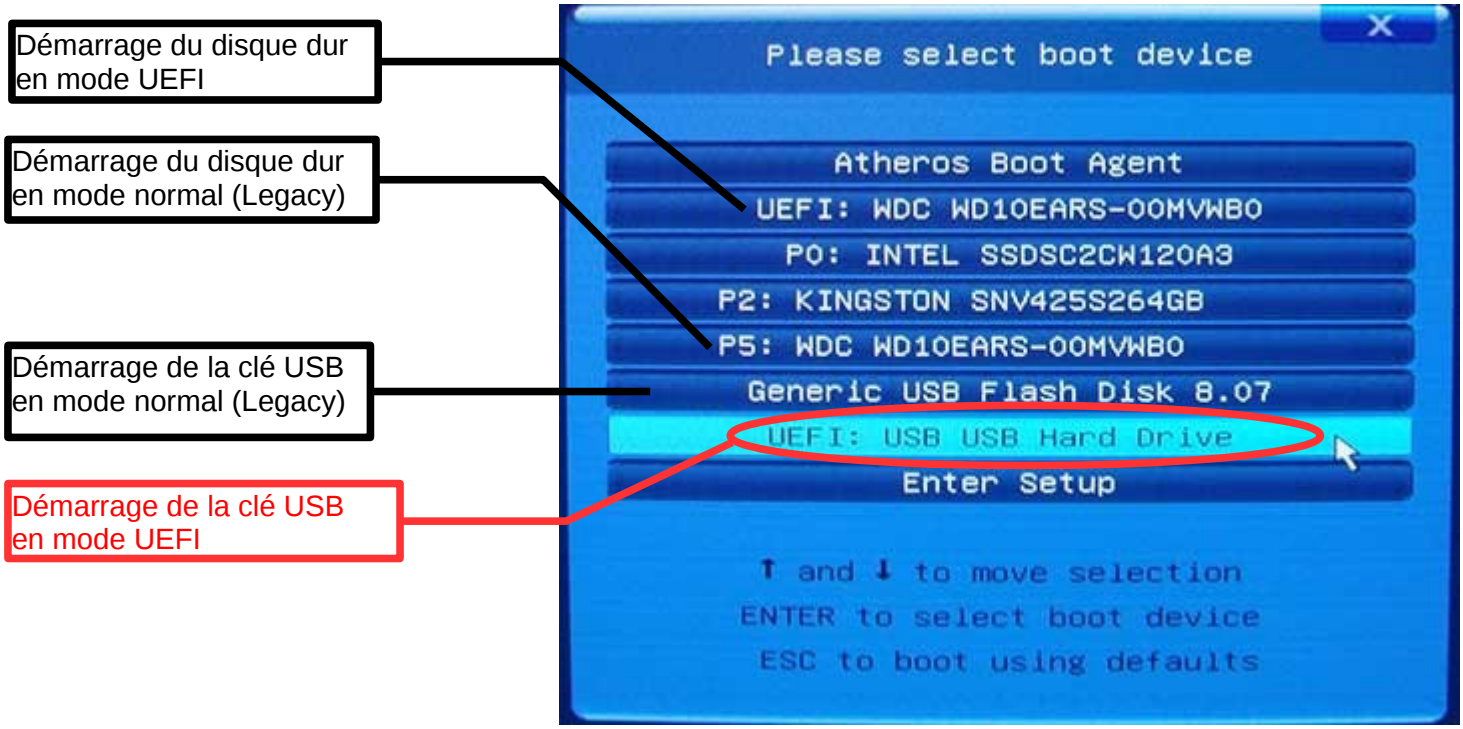
Contrairement au bios normal (qui utilise le format MBR), le bios UEFI utilise le nouveau format de partitionnement GPT.

Il faut vérifier si le disque dur est en partitionnement GPT, si ce n'est pas le cas (avec les disques neufs), il faut le convertir en GPT.

a) Booter sur Ubuntu 64 bits (obligatoire)

Seul une version 64 bits de Linux peut booter et s'installer sur un système UEFI.

Il faut faire attention à choisir le mode UEFI pour booter votre clé USB contenant Ubuntu.



Lorsque Ubuntu démarre en mode UEFI, le menu Grub s'affiche (voici l'image) :

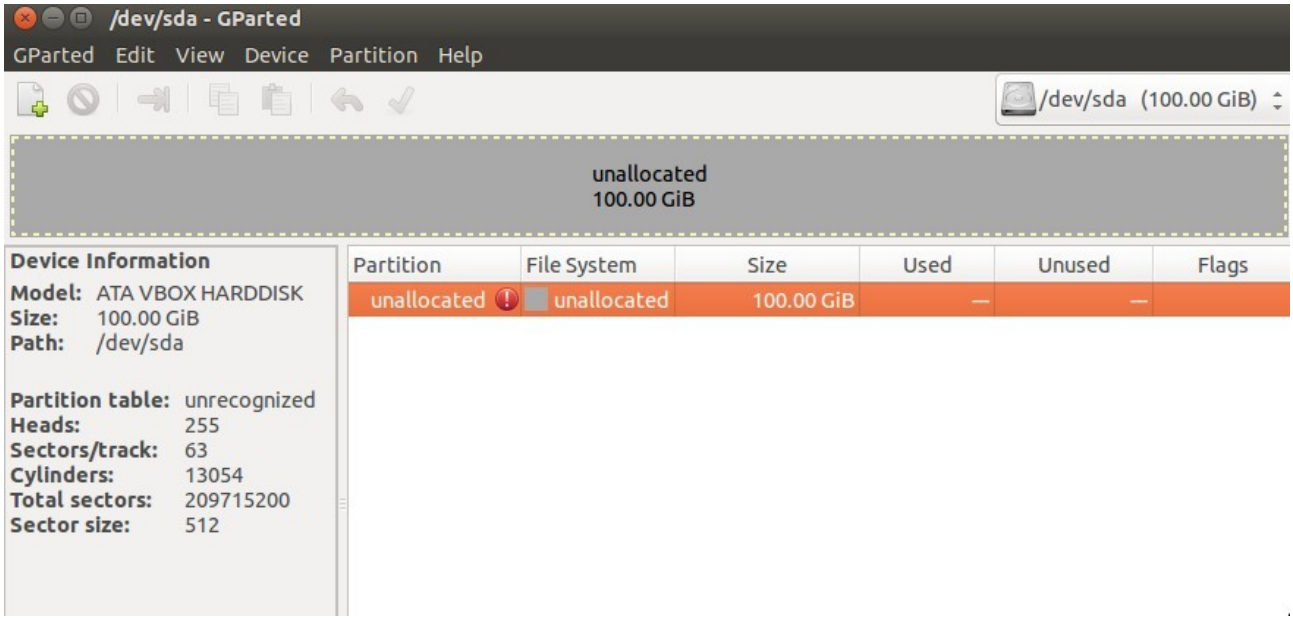
- Essayez Ubuntu sans l'installer

b) Ouvrir Gparted et convertir le disque dur en format GPT

- Ouvrez Gparted avec le lanceur rapide

- On peut visualiser les partitions qui sont présentes sur le disque dur.

- Dans ma capture il n'y a rien, la table de partition est inconnu car j'utilise une machine virtuelle.

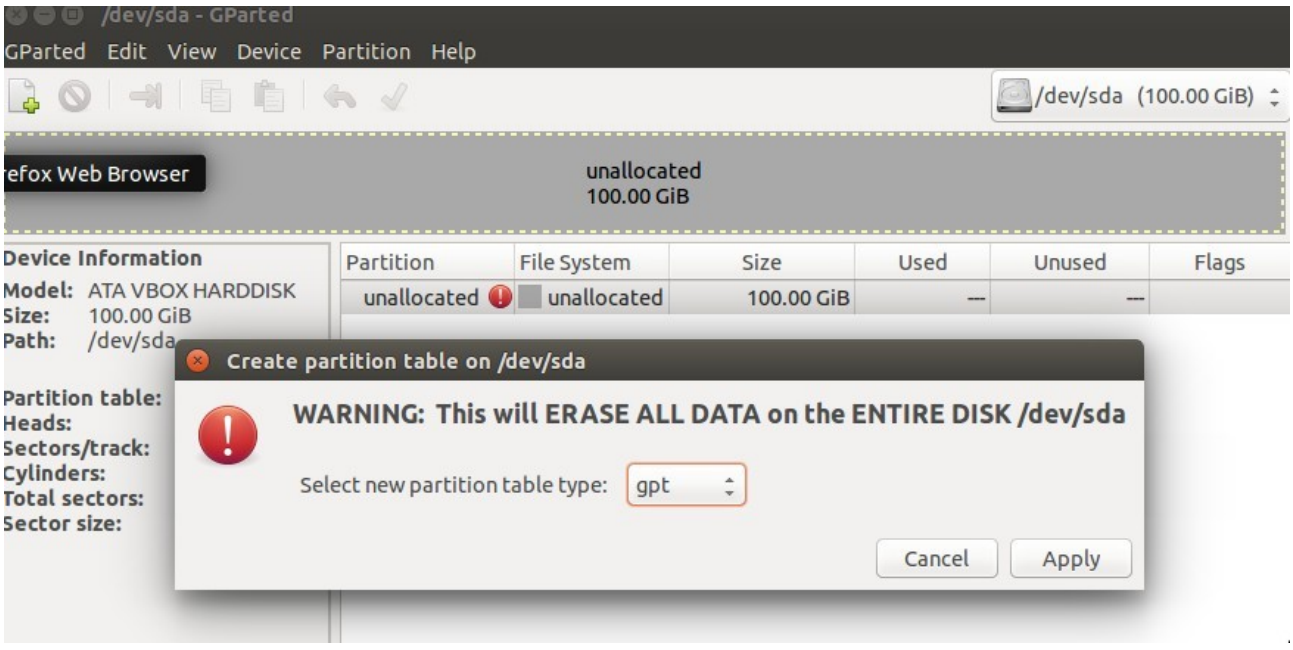


- Normalement votre disque dur est partitionné en MBR.

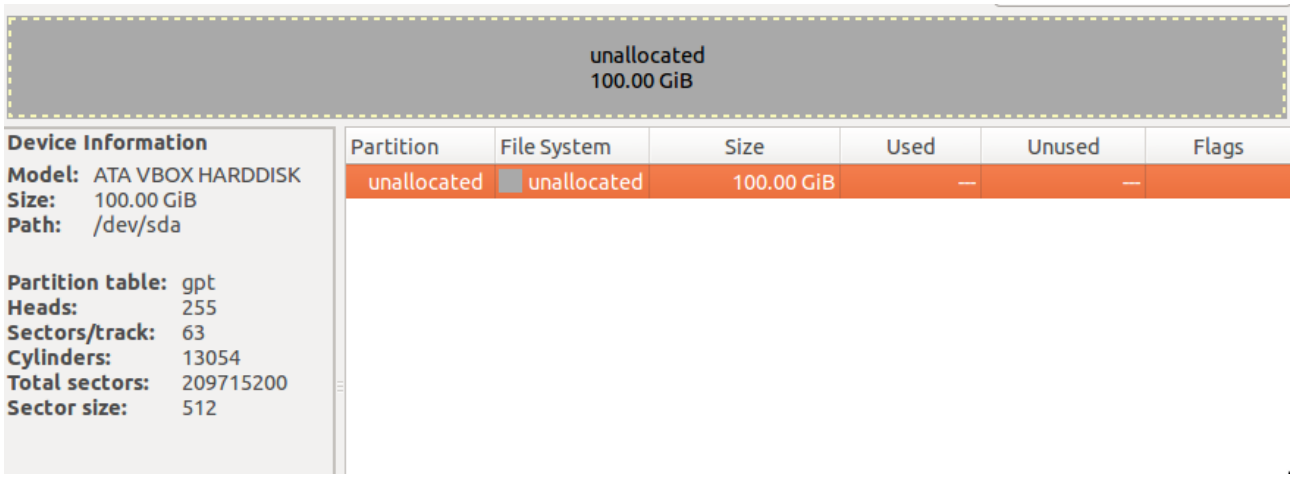
- Si votre disque est déjà en format GPT, suivez quand même la procédure, juste pour le fun =)

- Cliquez sur Device ---> Create a partition table
- Choisissez le format GPT pour la nouvelle table de partition du disque dur

TOUS LES FICHIERS SUR LE DISQUE SERONT PERDUS !!



Le disque utilise maintenant la table de partition GPT.



- Fermez la session live d'Ubuntu
- Rebootez de nouveau sur la clé usb en mode UEFI
- Vérifiez de nouveau avec Gparted que le disque est en format GPT (sans rien faire d'autre)

3] Installez maintenant Ubuntu

Poursuivez de la même façon l'installation. Allez voir la page 4 chapitre « Ubuntu seul (non-UEFI) » section n°5 et suivez les instructions.

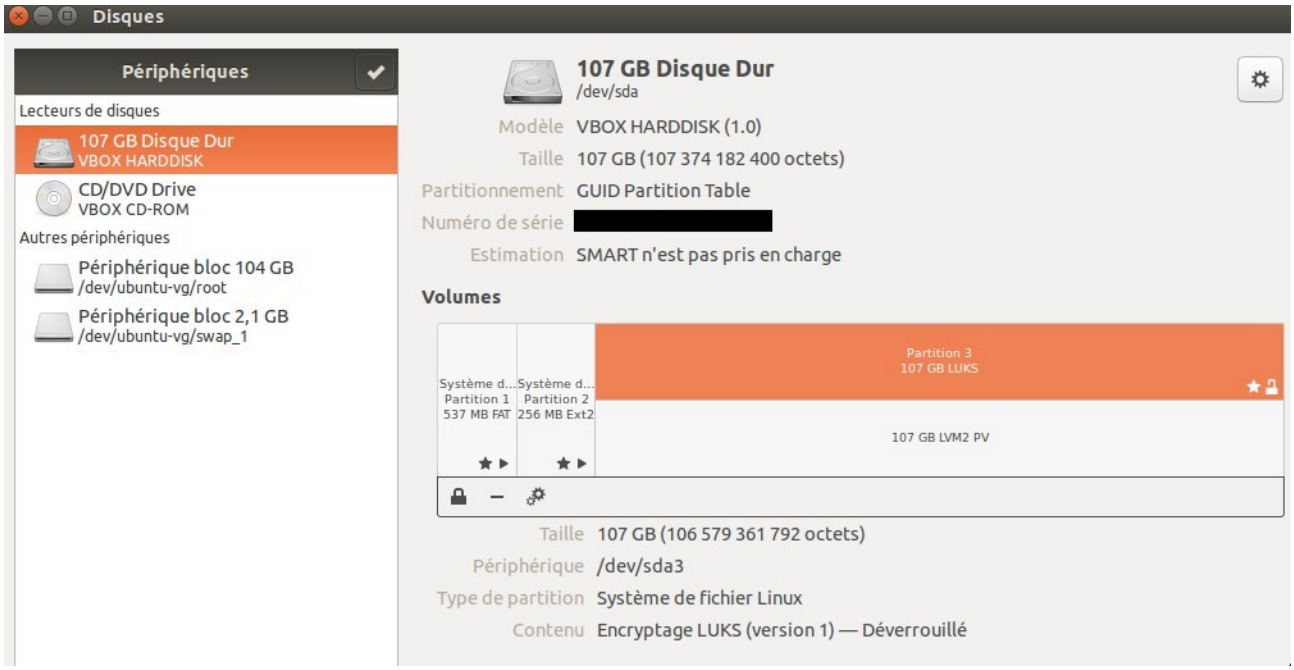
4] Une fois l'installation d'Ubuntu terminée

Vérifiez si Ubuntu s'est bien installé en mode UEFI (avant de sécuriser le système)

Dans un terminal copiez-collez puis faites entrée :
`[ -d /sys/firmware/efi ] && echo "Installé en mode EFI" || echo "Installé en mode classique"`

Ouvrez le logiciel Disques

- Vérifiez la table de partition → Elle doit être en format GPT



WINDOWS 7 + UBUNTU (non-UEFI)

ça ne finira jamais...