“avancé”

# LINUX AVANCÉ

formations.minet.net

Presented by: π & pwnsard

# Petits rappels

- touch - change file timestamps (créer un fichier vide)
- mkdir - **m**a**k**e **dir**ectories
- ls - **l**i**s**t directory contents
- pwd - **p**rint name of current/**w**orking **d**irectory
- cd - **c**hange **d**irectory
- rmdir - **r**e**m**ove empty **dir**ectories
- rm - **r**e**m**ove files or directories
- echo - display a line of text
- man - an interface to the system reference **man**uals
- cat - con**cat**enate files and print on the standard output
- cp - **c**o**p**y files and directories
- mv - **m**o**v**e (rename) files
- su - run a command with **su**bstitute user and group ID
- sudo - execute a command as another user (**su**bstitute **do**)

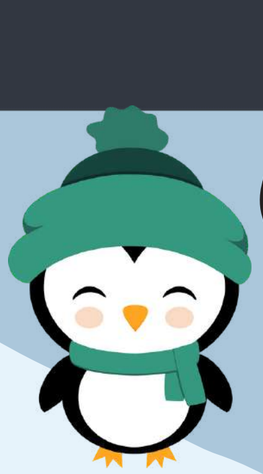
Des exemples ?
https://tldr.inbrowser.app/

# ps - report a snapshot of the current processes (**p**rocess **s**tatus).

```
root@hrtc:/# ps -Af
UID          PID    PPID  C STIME TTY          TIME CMD
root           1       0  0 Oct05 ?        00:00:09 /usr/lib/systemd/systemd --system --deserial
message+      82       1  0 Oct05 ?        00:00:02 @dbus-daemon --system --address=systemd: --n
root          84       1  0 Oct05 ?        00:00:00 /usr/lib/systemd/systemd-logind
root          87       1  0 Oct05 pts/0    00:00:00 /sbin/agetty -o -p -- \u --noclear --keep-ba
root          88       1  0 Oct05 tty1     00:00:00 /sbin/agetty -o -p -- \u --noclear - linux
root        1536       1  0 Oct05 ?        00:00:07 /usr/lib/systemd/systemd-journald
systemd+    2091       1  0 Oct05 ?        00:00:02 /usr/lib/systemd/systemd-resolved
root        7530       0  0 Oct05 pts/1    00:00:00 bash
root        7879    7530  0 04:18 pts/1    00:00:00 ps -Af
```

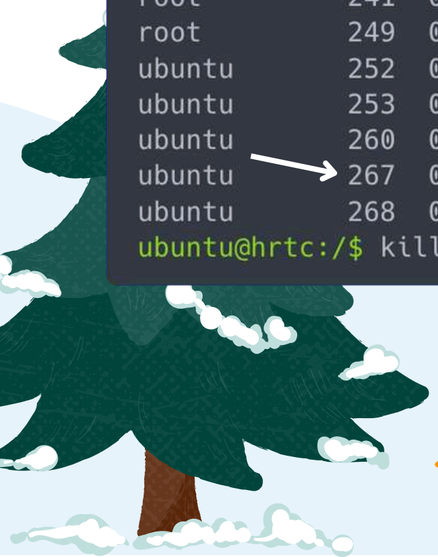
**1 processus = 1 PID**

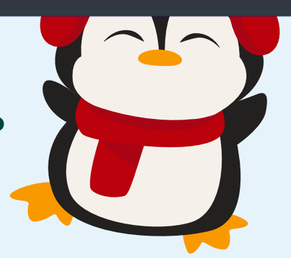
-A: show **A**ll, -f: show **f**ull



# kill - send a signal to a process

```
ubuntu@hrtc:/$ sleep 100 &
[1] 267
ubuntu@hrtc:/$ ps aux <- équivalent ps -Af
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.1  20864 11376 ?        Ss   20:33   0:00 /sbin/init
root          24  0.0  0.1  50076 14884 ?        S<s  20:33   0:00 /usr/lib/systemd/systemd-j
systemd+      73  0.0  0.1  21496 12444 ?        Ss   20:33   0:00 /usr/lib/systemd/systemd-r
message+      82  0.0  0.0   9612  4388 ?        Ss   20:33   0:00 @dbus-daemon --system --ad
root          84  0.0  0.0  17792  7572 ?        Ss   20:33   0:00 /usr/lib/systemd/systemd-l
root          87  0.0  0.0   2732  1560 pts/0    Ss+  20:33   0:00 /sbin/agetty -o -p -- \u -
root          88  0.0  0.0   2688  1548 tty1     Ss+  20:33   0:00 /sbin/agetty -o -p -- \u -
root         241  0.0  0.0   4296  3612 pts/2    Ss   20:42   0:00 bash
root         249  0.0  0.0   7204  3368 pts/2    S    20:42   0:00 su ubuntu
ubuntu       252  0.0  0.1  19676 10264 ?        Ss   20:42   0:00 /usr/lib/systemd/systemd -
ubuntu       253  0.0  0.0  21928  3220 ?        S    20:42   0:00 (sd-pam)
ubuntu       260  0.0  0.0   4732  3748 pts/2    S    20:42   0:00 bash
ubuntu       267  0.0  0.0   2696  1584 pts/2    S    20:46   0:00 sleep 100
ubuntu       268  0.0  0.0   8020  3796 pts/2    R+   20:47   0:00 ps aux
ubuntu@hrtc:/$ kill 267
```





# kill - send a signal to a process

```
ubuntu@hrtc:~$ kill -L
 1) SIGHUP       2) SIGINT       3) SIGQUIT      4) SIGILL       5) SIGTRAP
 6) SIGABRT      7) SIGBUS       8) SIGFPE       9) SIGKILL     10) SIGUSR1
11) SIGSEGV     12) SIGUSR2     13) SIGPIPE     14) SIGALRM     15) SIGTERM
16) SIGSTKFLT   17) SIGCHLD     18) SIGCONT     19) SIGSTOP     20) SIGTSTP
21) SIGTTIN     22) SIGTTOU     23) SIGURG      24) SIGXCPU     25) SIGXFSZ
26) SIGVTALRM   27) SIGPROF     28) SIGWINCH    29) SIGIO       30) SIGPWR
31) SIGSYS      34) SIGRTMIN    35) SIGRTMIN+1  36) SIGRTMIN+2  37) SIGRTMIN+3
38) SIGRTMIN+4  39) SIGRTMIN+5  40) SIGRTMIN+6  41) SIGRTMIN+7  42) SIGRTMIN+8
43) SIGRTMIN+9  44) SIGRTMIN+10 45) SIGRTMIN+11 46) SIGRTMIN+12 47) SIGRTMIN+13
48) SIGRTMIN+14 49) SIGRTMIN+15 50) SIGRTMAX-14 51) SIGRTMAX-13 52) SIGRTMAX-12
53) SIGRTMAX-11 54) SIGRTMAX-10 55) SIGRTMAX-9  56) SIGRTMAX-8  57) SIGRTMAX-7
58) SIGRTMAX-6  59) SIGRTMAX-5  60) SIGRTMAX-4  61) SIGRTMAX-3  62) SIGRTMAX-2
63) SIGRTMAX-1  64) SIGRTMAX
ubuntu@hrtc:~$ kill -9 267
```

TUER C'EST GRAVE COOL

-L: **L**ist

# htop - interactive process viewer

```
  0[                                                    0.0%] Tasks: 36, 76 thr, 75 kthr; 1 running
  1[                                                    0.0%] Load average: 0.07 0.03 0.00
  2[|                                                   0.7%] Uptime: 3 days, 23:18:06
  3[                                                    0.0%]
Mem[||||||||||||||                                424M/7.75G]
Swp[                                                 0K/975M]

  Main   I/O
    PID△USER       PRI  NI  VIRT   RES   SHR S  CPU% MEM%   TIME+  Command
      1 root        20   0  163M 12352  9228 S   0.0  0.2  0:06.18 /sbin/init
    231 root        20   0 74396 41420 38148 S   0.0  0.5  0:04.25   ├─ /lib/systemd/systemd-journald
    264 root        20   0 26904  6272  4632 S   0.0  0.1  0:00.69   ├─ /lib/systemd/systemd-udevd
    460 messagebus  20   0 28452  4756  4140 S   0.0  0.1  0:03.82   ├─ /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --system
    462 root        20   0 1276M 79356 51212 S   0.0  1.0  1:08.21   ├─ /usr/bin/gitlab-runner run --config /etc/gitlab-runner/config.toml --working-d
    471 root        20   0 1276M 79356 51212 S   0.0  1.0  0:08.71   │   ├─ /usr/bin/gitlab-runner run --config /etc/gitlab-runner/config.toml --workin
    473 root        20   0 1276M 79356 51212 S   0.0  1.0  0:13.82   │   ├─ /usr/bin/gitlab-runner run --config /etc/gitlab-runner/config.toml --workin
    474 root        20   0 1276M 79356 51212 S   0.0  1.0  0:00.01   │   ├─ /usr/bin/gitlab-runner run --config /etc/gitlab-runner/config.toml --workin
    475 root        20   0 1276M 79356 51212 S   0.0  1.0  0:11.87   │   ├─ /usr/bin/gitlab-runner run --config /etc/gitlab-runner/config.tom
    484 root        20   0 1276M 79356 51212 S   0.0  1.0  0:11.26   │   ├─ /usr/bin/gitlab-runner run --config /etc/gitlab-runner/config.t
    491 root        20   0 1276M 79356 51212 S   0.0  1.0  0:11.10   │   ├─ /usr/bin/gitlab-runner run --config /etc/gitlab-runner/config.t
    495 root        20   0 1276M 79356 51212 S   0.0  1.0  0:00.00   │   ├─ /usr/bin/gitlab-runner run --config /etc/gitlab-runn onfig.t
    [illegible] root 20  0 1276M 79356 51212 S   0.0  1.0  0:11.12   │   └─ /usr/bin/gitlab-runner run --config /etc/gitlab-run nfig.t
    [illegible]     20   0 80380  3624  3352 S   0.7  0.0  3:59.82   ├─ /usr/sbin/qemu-ga
    [illegible]     20   0 80380  3624  3352 S   0.0  0.0  0:00.00   │   └─ /usr/sbin/qemu-ga
    [illegible]     20   0 31244 12168 10004 S   0.0  0.1  0:00.79   ├─ /usr/sbin/sssd -i --logger=files
    [illegible]     20   0 46788 28892 15136 S   0.0  0.4  0:28.47   │   ├─ /usr/libexec/sssd/sssd_be --domain LDAP --uid 0 ger=
F1[illegible]etup F3SearchF4FilterF5List  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
[illegible]x]  1:VPN  2:ansible  3:zsh  4:zsh  5:zsh- 6:ssh* 9:zsh                                  "device- 23:15
```

A daemon is a service process that runs in the background

# systemd - systemd system and service manager
# systemctl - Control the systemd system and service manager

```
root@hrtc:/# systemctl
  UNIT                                      LOAD   ACTIVE     SUB       DESCRIPTION
  ssh.service                               loaded failed     failed    OpenBSD Secure Shell server
  systemd-binfmt.service                    loaded active     exited    Set Up Additional Binary Formats
  systemd-journal-catalog-update.service    loaded active     exited    Rebuild Journal Catalog
  systemd-journal-flush.service             loaded active     exited    Flush Journal to Persistent Storage
  systemd-journald.service                  loaded active     running   Journal Service
```

```
root@hrtc:/# systemctl --failed
  UNIT        LOAD   ACTIVE SUB    DESCRIPTION
● ssh.service loaded failed failed OpenBSD Secure Shell server
● ssh.socket  loaded failed failed OpenBSD Secure Shell server socket
```

```
root@hrtc:/# systemctl restart ssh
Job for ssh.service failed because the control process exited with error code.
See "systemctl status ssh.service" and "journalctl -xeu ssh.service" for details.
```

```
root@hrtc:/# systemctl status ssh
× ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: failed (Result: exit-code) since Mon 2025-10-06 04:42:16 UTC; 1min 38s ago
TriggeredBy: × ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
        CPU: 6ms

Oct 06 04:42:16 hrtc systemd[1]: ssh.service: Scheduled restart job, restart counter is at 5.
Oct 06 04:42:16 hrtc systemd[1]: ssh.service: Start request repeated too quickly.
Oct 06 04:42:16 hrtc systemd[1]: ssh.service: Failed with result 'exit-code'.
Oct 06 04:42:16 hrtc systemd[1]: Failed to start ssh.service - OpenBSD Secure Shell server
```

# journalctl - Print log entries from the systemd journal

```
root@hrtc:/# journalctl -eu ssh
...
Oct 06 04:42:15 hrtc systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Oct 06 04:42:15 hrtc sshd[8062]: /etc/ssh/sshd_config: line 12: Bad configuration option: Minet
Oct 06 04:42:15 hrtc sshd[8062]: /etc/ssh/sshd_config: terminating, 1 bad configuration options
Oct 06 04:42:15 hrtc systemd[1]: ssh.service: Control process exited, code=exited, status=255/EXCEPTION
Oct 06 04:42:15 hrtc systemd[1]: ssh.service: Failed with result 'exit-code'.
Oct 06 04:42:15 hrtc systemd[1]: Failed to start ssh.service - OpenBSD Secure Shell server.
```

**-e**: **e**nd, -**u**: systemd **u**nit

```
root@hrtc:/# cat /etc/ssh/sshd_config

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information

Include /etc/ssh/sshd_config.d/*.conf

Port 22
ListenAddress 0.0.0.0
ListenAddress ::

Minet broke my config

UsePAM yes
```

```
root@hrtc:/# systemctl cat ssh
# /usr/lib/systemd/system/ssh.service
[Unit]
Description=OpenBSD Secure Shell server
Documentation=man:sshd(8) man:sshd_config(5)
After=network.target auditd.service
ConditionPathExists=!/etc/ssh/sshd_not_to_be_run

[Service]
EnvironmentFile=-/etc/default/ssh
ExecStartPre=/usr/sbin/sshd -t
ExecStart=/usr/sbin/sshd -D $SSHD_OPTS
ExecReload=/usr/sbin/sshd -t
ExecReload=/bin/kill -HUP $MAINPID
KillMode=process
Restart=on-failure
RestartPreventExitStatus=255
Type=notify
RuntimeDirectory=sshd
RuntimeDirectoryMode=0755

[Install]
WantedBy=multi-user.target
Alias=sshd.service
```

```
root@hrtc:/# systemctl restart ssh
root@hrtc:/# systemctl stop ssh
root@hrtc:/# systemctl start ssh
root@hrtc:/# systemctl disable ssh
root@hrtc:/# systemctl enable ssh
```

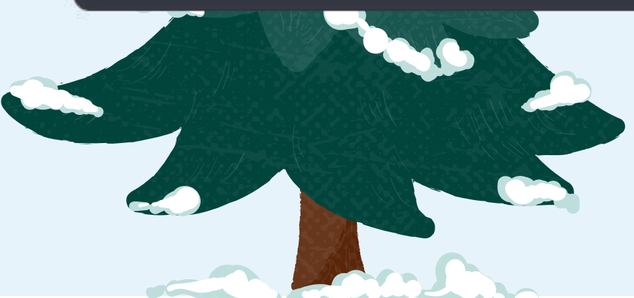
chmod - **ch**ange file **mod**e bits

chown - **ch**ange file **own**er and group

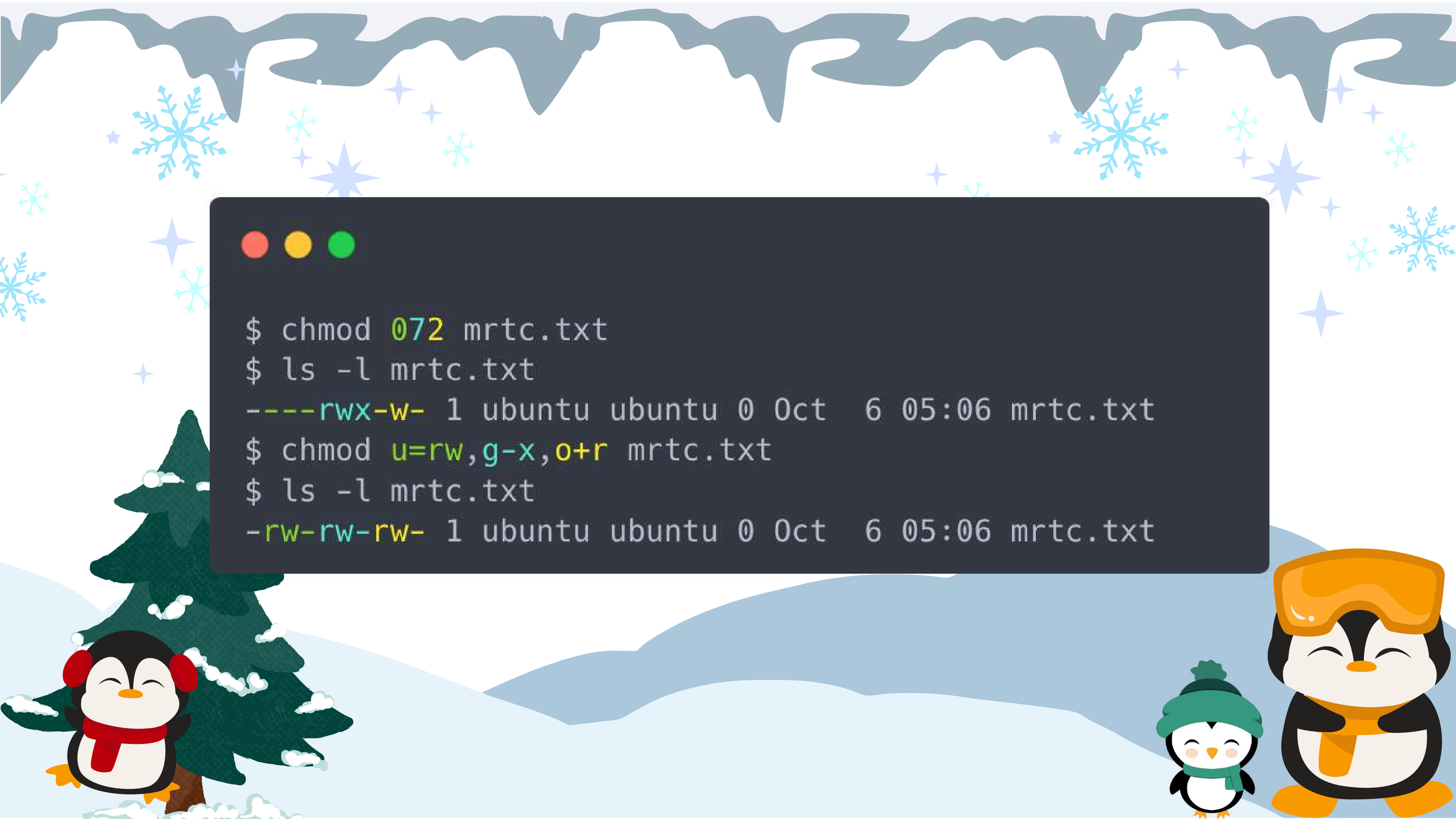
```
ubuntu@hrtc:~$ touch mrtc.txt
ubuntu@hrtc:~$ ls -l mrtc.txt
-rw-rw-r-- 1 ubuntu ubuntu 0 Oct  6 05:06 mrtc.txt
ubuntu@hrtc:~$ chmod 123 mrtc.txt
ubuntu@hrtc:~$ ls -l mrtc.txt
---x-w--wx 1 ubuntu ubuntu 0 Oct  6 05:06 mrtc.txt
ubuntu@hrtc:~$ sudo chown mrtc mrtc.txt
ubuntu@hrtc:~$ ls -l mrtc.txt
---x-w--wx 1 mrtc adm 0 Oct  6 05:06 mrtc.txt
```

-rw-rw-r-- ??

**r**ead ?
**w**rite ?
e**x**ecute ??




$ chmod 777 mrtc.txt
-rwxrwxrwx
111111111
7 7 7
user (owner)
group
others
$ chmod 664 mrtc.txt
-rw-rw-r--
110110100
6 6 4
(indique le type du fichier)


$ chmod 072 mrtc.txt
$ ls -l mrtc.txt
----rwx-w- 1 ubuntu ubuntu 0 Oct  6 05:06 mrtc.txt
$ chmod u=rw,g-x,o+r mrtc.txt
$ ls -l mrtc.txt
-rw-rw-rw- 1 ubuntu ubuntu 0 Oct  6 05:06 mrtc.txt

# Les paquets

## I. Type tout con : l'executable

**$PATH est ton ami !**

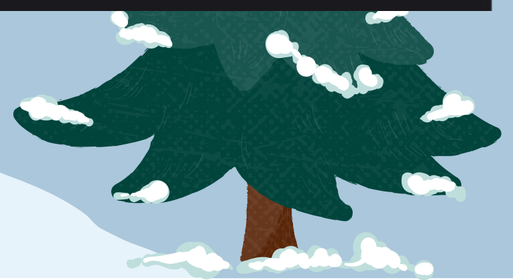
*Pour la persistence : .bashrc*

**Mais pas mal d'inconvénients :(**

**=> .deb et apt**

# I. Type tout con : l'executable

```
antoine@framework:~/hello$ cat main.c
#include <stdio.h>
int main() {
   // printf() displays the string inside quotation
   printf("MRTC\n");
   return 0;
}
antoine@framework:~/hello$ gcc main.c -o mrtc
antoine@framework:~/hello$ ./mrtc
MRTC
antoine@framework:~/hello$ cd ..
antoine@framework:~$ ./mrtc
bash: ./mrtc: Aucun fichier ou dossier de ce nom
antoine@framework:~$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/sbin:/bin
antoine@framework:~$ cd hello/
antoine@framework:~/hello$ pwd
/var/home/antoine/toolboxes/debian/hello
antoine@framework:~/hello$ cd ..
antoine@framework:~$ export PATH=$PATH:/var/home/antoine/toolboxes/debian/hello
antoine@framework:~$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/sbin:/bin:/var/home/antoine/toolboxes
/debian/hello
antoine@framework:~$ mrtc
MRTC
```



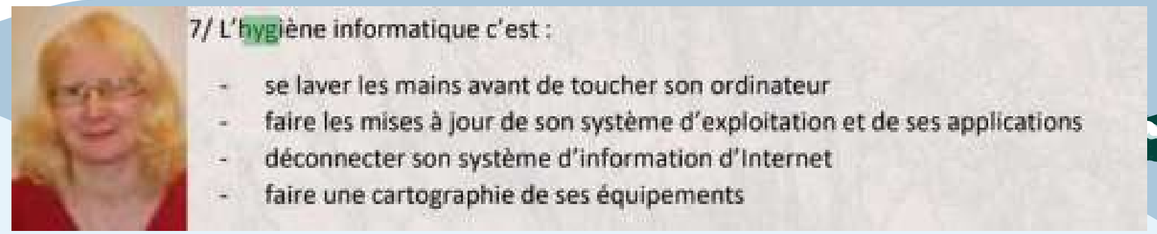
# Les paquets

# II. Gérer tout plein d'executables : package manager

apt est ton ami !

sources ????? : /etc/apt/sources.list.d

sudo apt update
sudo apt upgrade
sudo apt install ...
sudo apt remove ...



# Les paquets

```
antoine@framework:~$ sudo apt update
Atteint : 1 http://deb.debian.org/debian trixie InRelease
Atteint : 2 http://deb.debian.org/debian trixie-updates InRelease
Atteint : 3 http://deb.debian.org/debian-security trixie-security InRelease
Réception de : 4 http://deb.debian.org/debian trixie/main Translation-fr [3 137 kB]
3 137 ko réceptionnés en 1s (3 472 ko/s)
3 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.
antoine@framework:~$ sudo apt upgrade
Mis à jour :
  libssl3t64  openssl  openssl-provider-legacy

Sommaire :
  Mise à niveau de : 3. Installation de : 0Supprimé : 0. Non mis à jour : 0
Taille du téléchargement : 4 238 kB
  Espace nécessaire : 0 B / 116 GB disponible

Continuer ? [O/n] O
Réception de : 1 http://deb.debian.org/debian-security trixie-security/main amd64 openssl-provider-legacy amd64 3.5.1-1+deb13u1 [307 kB]
Réception de : 2 http://deb.debian.org/debian-security trixie-security/main amd64 libssl3t64 amd64 3.5.1-1+deb13u1 [2 437 kB]
Réception de : 3 http://deb.debian.org/debian-security trixie-security/main amd64 openssl amd64 3.5.1-1+deb13u1 [1 494 kB]
4 238 ko réceptionnés en 1s (7 575 ko/s)
(Lecture de la base de données... 21254 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../openssl-provider-legacy_3.5.1-1+deb13u1_amd64.deb ...
Dépaquetage de openssl-provider-legacy (3.5.1-1+deb13u1) sur (3.5.1-1) ...
Paramétrage de openssl-provider-legacy (3.5.1-1+deb13u1) ...
(Lecture de la base de données... 21254 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../libssl3t64_3.5.1-1+deb13u1_amd64.deb ...
Dépaquetage de libssl3t64:amd64 (3.5.1-1+deb13u1) sur (3.5.1-1) ...
Paramétrage de libssl3t64:amd64 (3.5.1-1+deb13u1) ...
(Lecture de la base de données... 21254 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../openssl_3.5.1-1+deb13u1_amd64.deb ...
Dépaquetage de openssl (3.5.1-1+deb13u1) sur (3.5.1-1) ...
Paramétrage de openssl (3.5.1-1+deb13u1) ...
Traitement des actions différées (« triggers ») pour man-db (2.13.1-1) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.41-12) ...
antoine@framework:~$
```

# Les paquets

# III. Le turfu

snap n'est pas ton ami :(

Flatpak c'est mieux


# SSH

***ssh-keygen***
***.ssh/authorized_keys***

# BLOOKEEEET

voilà voilà

# MAINTENANT TP

https://wiki.minet.net/fr/mini_tp_formation/linux/pipes

**Presented by: des gens**