


Introducción a Linux

Cuentas de usuario

Cuentas de usuario


/etc/passwd



```
geoclue:x:119:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:120:65534::/run/gnome-initial-setup:/bin/false
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
student:x:1000:1000:LF Student,,,:/home/student:/bin/bash
sshd:x:122:65534::/run/sshd:/usr/sbin/nologin
```

(usuario: contraseña: UID: GID: descripción: directorio de inicio: Shell predeterminado)

/etc/group



```
sudo:x:27:student
ssh:x:115:
lpadmin:x:116:student
scanner:x:118:saned
gdm:x:125:
student:x:1000:
```

Manipular con
`useradd`
`userdel`

Tipos de cuentas de usuario

Tipos de cuenta

- root
- system (sistema)
- Normal
- Network (red)

```
student@ubuntu: ~  
student@ubuntu:~$ last  
student  tty7          :0                Thu Dec 15 11:51    gone - no logout  
student  tty7          :0                Thu Dec 15 11:49 - 11:51    (00:01)  
reboot   system boot    4.4.0-53-generic  Thu Dec 15 11:48    still running  
student  tty7          :0                Wed Dec 14 09:39 - down    (08:29)  
reboot   system boot    4.4.0-53-generic  Wed Dec 14 09:39 - 18:09    (08:29)  
student  tty7          :0                Mon Dec 12 09:35 - crash   (2+00:03)  
reboot   system boot    4.4.0-53-generic  Mon Dec 12 09:35 - 18:09    (2+08:34)  
student  tty7          :0                Mon Dec 12 09:26 - down    (00:07)  
reboot   system boot    4.9.0            Mon Dec 12 09:26 - 09:34    (00:07)  
student  tty7          :0                Mon Dec 12 09:26 - crash   (00:00)  
reboot   system boot    4.4.0-43-generic  Mon Dec 12 09:25 - 09:34    (00:08)  
student  tty7          :0                Mon Dec 12 09:00 - crash   (00:25)  
reboot   system boot    4.4.0-43-generic  Mon Dec 12 08:51 - 09:34    (00:43)  
student  tty7          :0                Fri Dec 9 13:09 - crash   (2+19:41)  
student  tty7          :0                Fri Dec 9 12:33 - 12:33    (00:00)  
student  tty2          :0                Fri Dec 9 12:32 - crash   (2+20:19)  
student  tty7          :0                Fri Dec 9 11:42 - 12:31    (00:49)  
reboot   system boot    4.4.0-43-generic  Fri Dec 9 11:42 - 09:34    (2+21:52)  
student  tty7          :0                Wed Dec 7 14:11 - crash   (1+21:30)  
  
wtmp begins Wed Dec 7 14:11:29 2016  
student@ubuntu:~$
```

La cuenta root

¡mucho cuidado!



#



Introducción a Linux

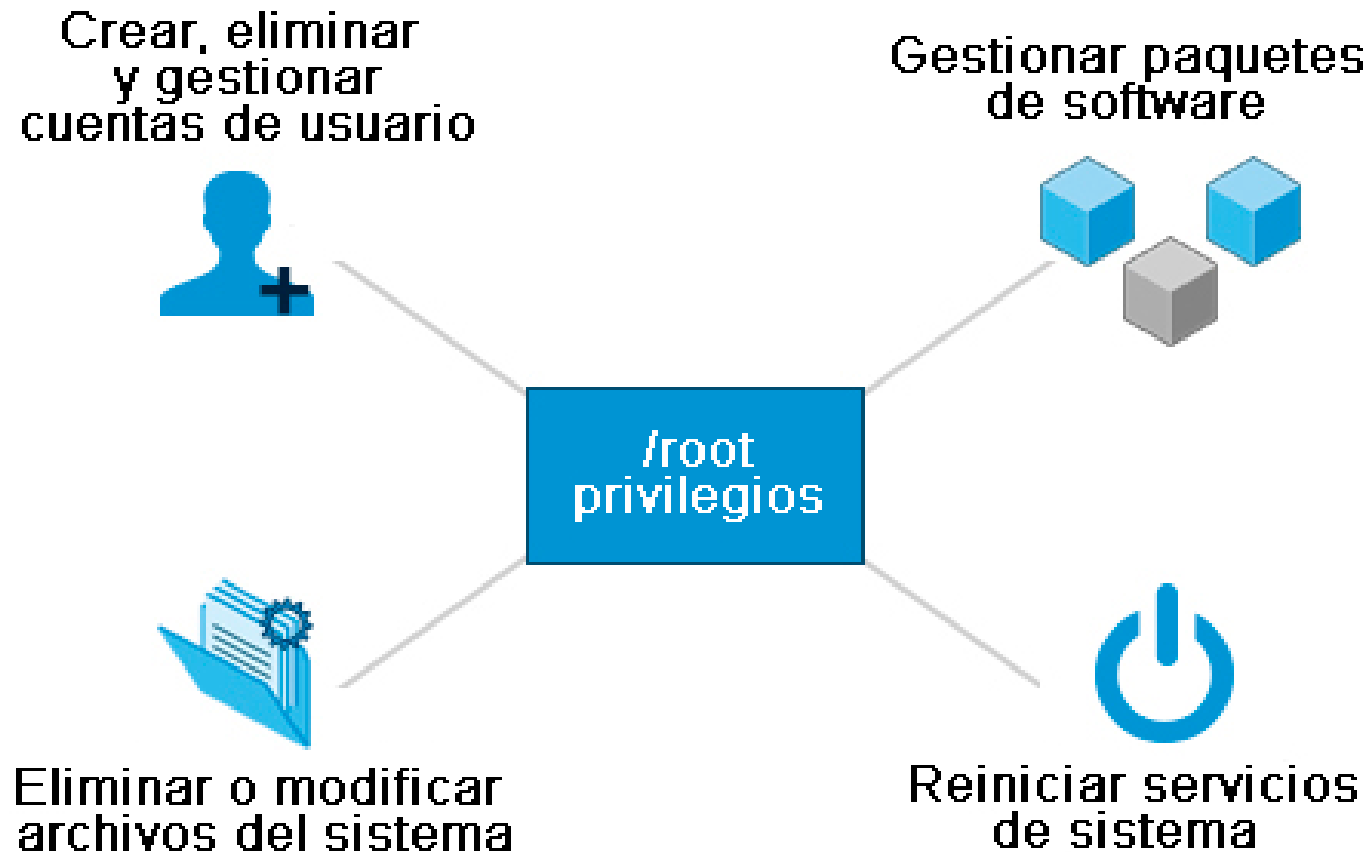
Cuentas de usuario



Introducción a Linux

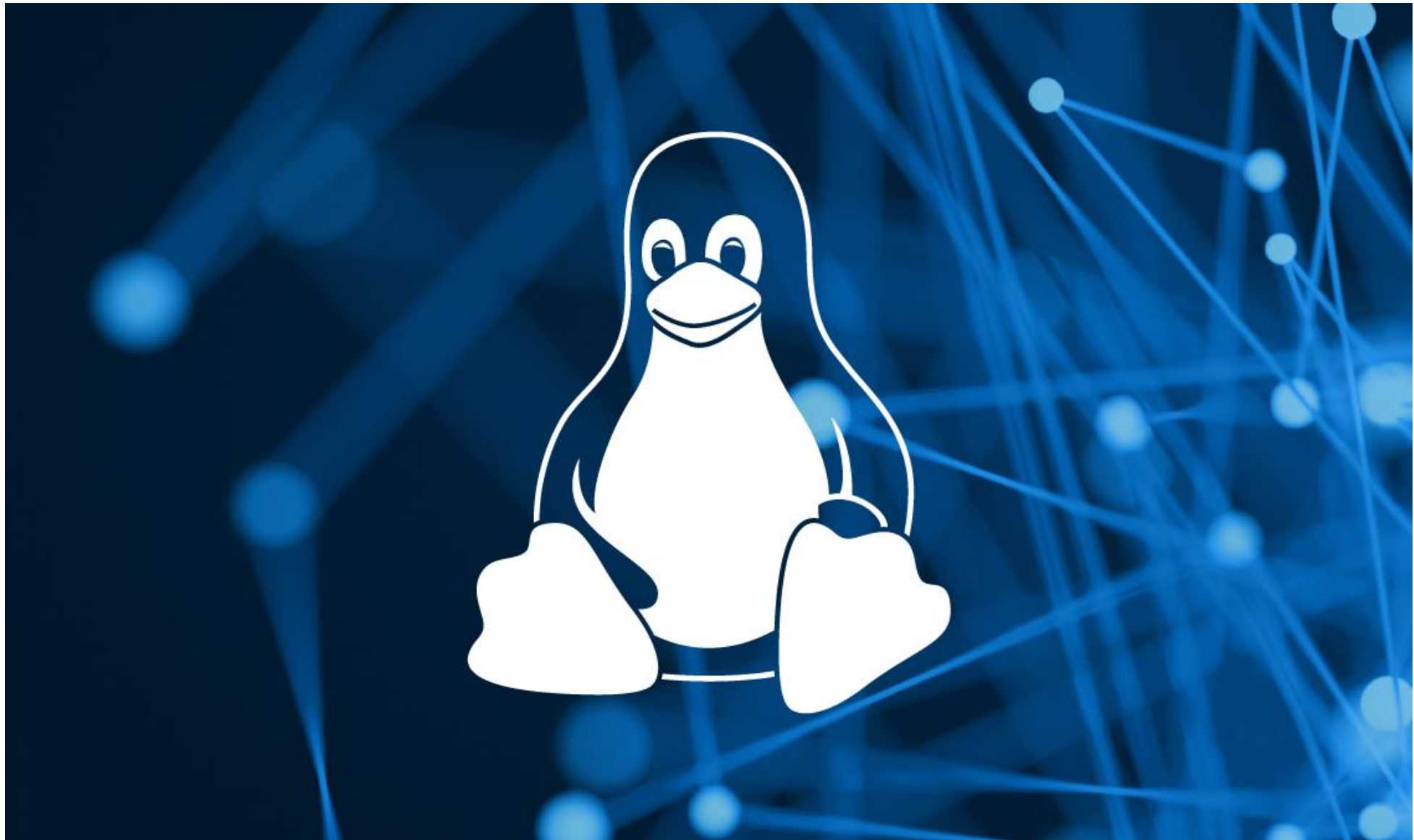
Operaciones que requieren privilegios root

Operaciones con privilegios root



Operaciones que no requieren privilegios root

Operaciones que no requieren privilegios de root	Ejemplos de esta operación
Ejecución de un cliente de red	Compartir un archivo a través de la red
Uso de dispositivos como impresoras	Impresión a través de la red
Operaciones en archivos a los que el usuario tiene los permisos adecuados para acceder	Acceso a los archivos a los que tiene acceso o comparte datos a través de la red
Ejecución de aplicaciones con SUID de root	Ejecución de programas tales como passwd



Introducción a Linux

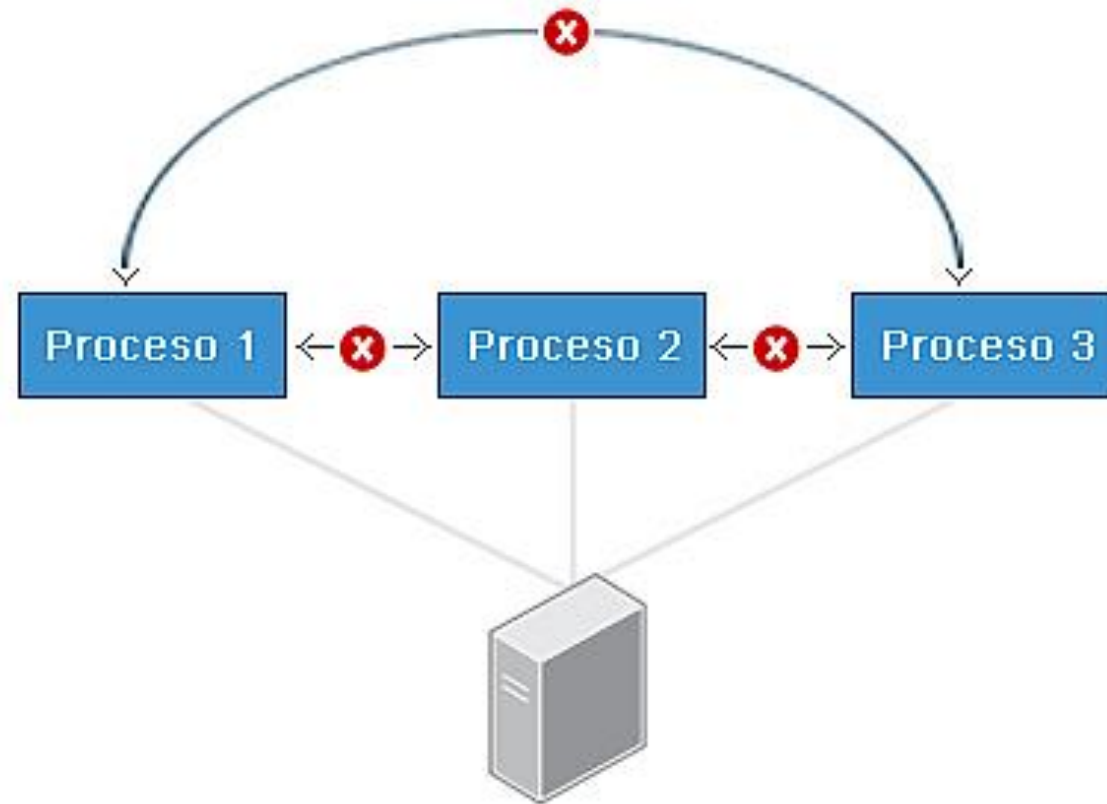
Operaciones que requieren privilegios root



Introducción a Linux

Aislamiento de procesos y limitaciones acceso al hardware

Aislamiento de procesos



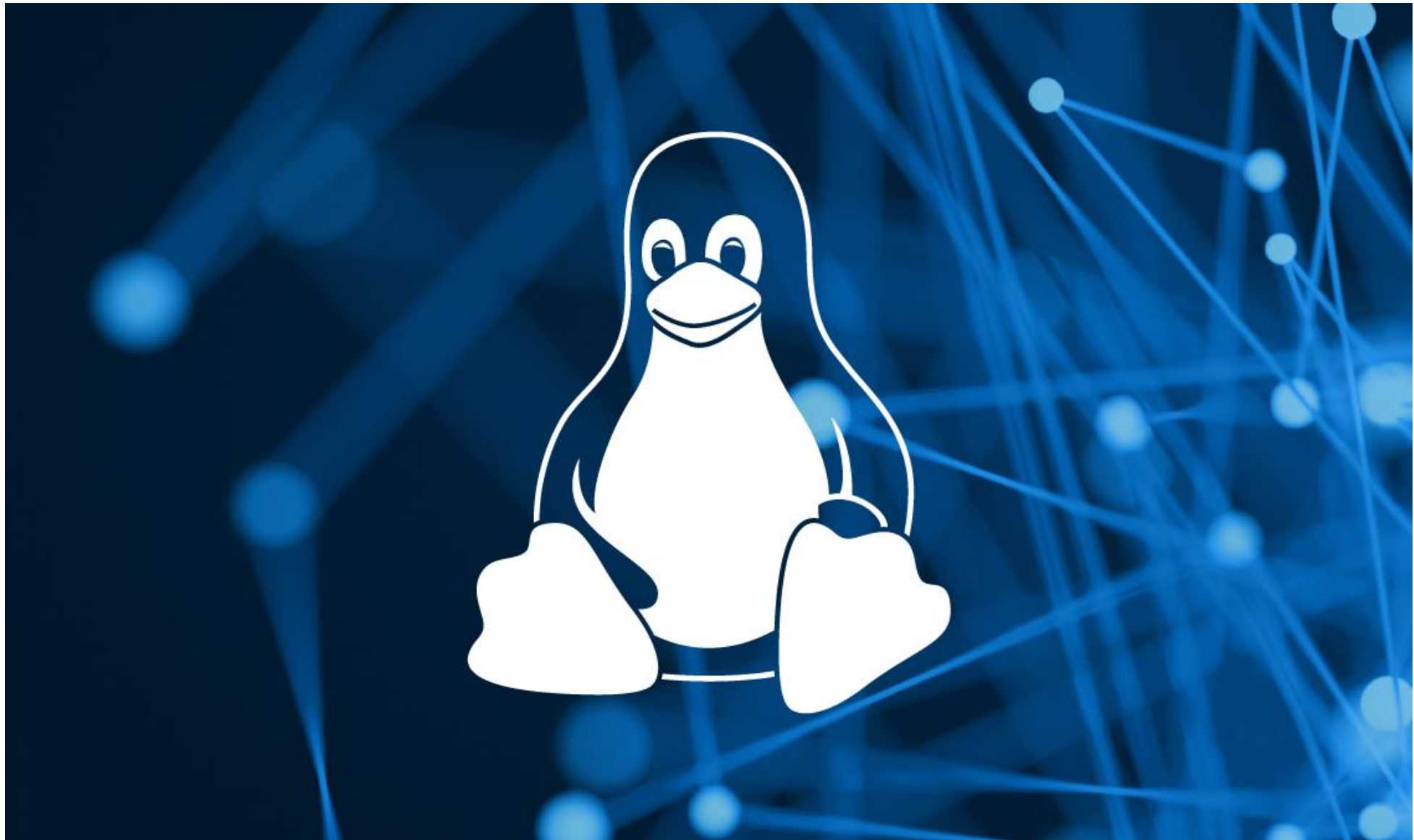
Accesso al hardware

```
File Edit View Search Terminal Help
c7:/etc>cd /dev
c7:/dev>ls -l /dev/sd*
brw-rw---- 1 root disk 8,  0 Dec 21 07:57 /dev/sda
brw-rw---- 1 root disk 8,  1 Dec 21 07:57 /dev/sda1
brw-rw---- 1 root disk 8,  2 Dec 21 07:57 /dev/sda2
brw-rw---- 1 root disk 8,  3 Dec 21 07:57 /dev/sda3
brw-rw---- 1 root disk 8,  5 Dec 21 07:57 /dev/sda5
brw-rw---- 1 root disk 8,  6 Dec 21 07:57 /dev/sda6
brw-rw---- 1 root disk 8, 16 Dec 21 07:57 /dev/sdb
brw-rw---- 1 root disk 8, 17 Dec 21 07:57 /dev/sdb1
brw-rw---- 1 root disk 8, 18 Dec 21 07:57 /dev/sdb2
brw-rw---- 1 root disk 8, 21 Dec 21 07:57 /dev/sdb5
brw-rw---- 1 root disk 8, 22 Dec 21 07:57 /dev/sdb6
brw-rw---- 1 root disk 8, 23 Dec 21 07:57 /dev/sdb7
c7:/dev>
```



Introducción a Linux

Aislamiento de procesos y limitaciones acceso al hardware



Introducción a Linux

Trabajando con contraseñas

Como se almacenan las contraseñas

Sistema antiguo

Información de contraseña



/etc/passwd
(fácil de crackear)

Sistema moderno

Información de contraseña en el archivo accesible solo para el root



/etc/shadow




Usuario root

```
student:x:1000:1000:LF Student,,,:/home/student:/bin/bash
```

(usuario: contraseña: UID: GID: descripción: directorio de inicio: Shell predeterminado)


Como se almacenan las contraseñas

/etc/passwd



```
geoclue:x:119:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:120:65534::/run/gnome-initial-setup:/bin/false
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
student:x:1000:1000:LF Student,,,:/home/student:/bin/bash
sshd:x:122:65534::/run/sshd:/usr/sbin/nologin
```


/etc/group



```
sudo:x:27:student
ssh:x:115:
lpadmin:x:116:student
scanner:x:118:saned
gdm:x:125:
student:x:1000:
```

(usuario:contraseña:UID:GID:descripción:directorio de inicio:Shell predeterminado)

/etc/shadow



```
geoclue*:18113:0:99999:7:::
gnome-initial-setup*:18113:0:99999:7:::
gdm*:18113:0:99999:7:::
student:$1$3SNnYNvv$JsHN99jiKMSmZWWyKBmXn0:18252:0:99999:7:::
sshd*:18252:0:99999:7:::
```

(usuario:contraseña cifrada:días ultimo cambio:días entre cambios:
días validez: días aviso: días para eliminar: fecha caducidad)

Algoritmo de contraseña

Protección de contraseñas

File Edit View Search Terminal Help

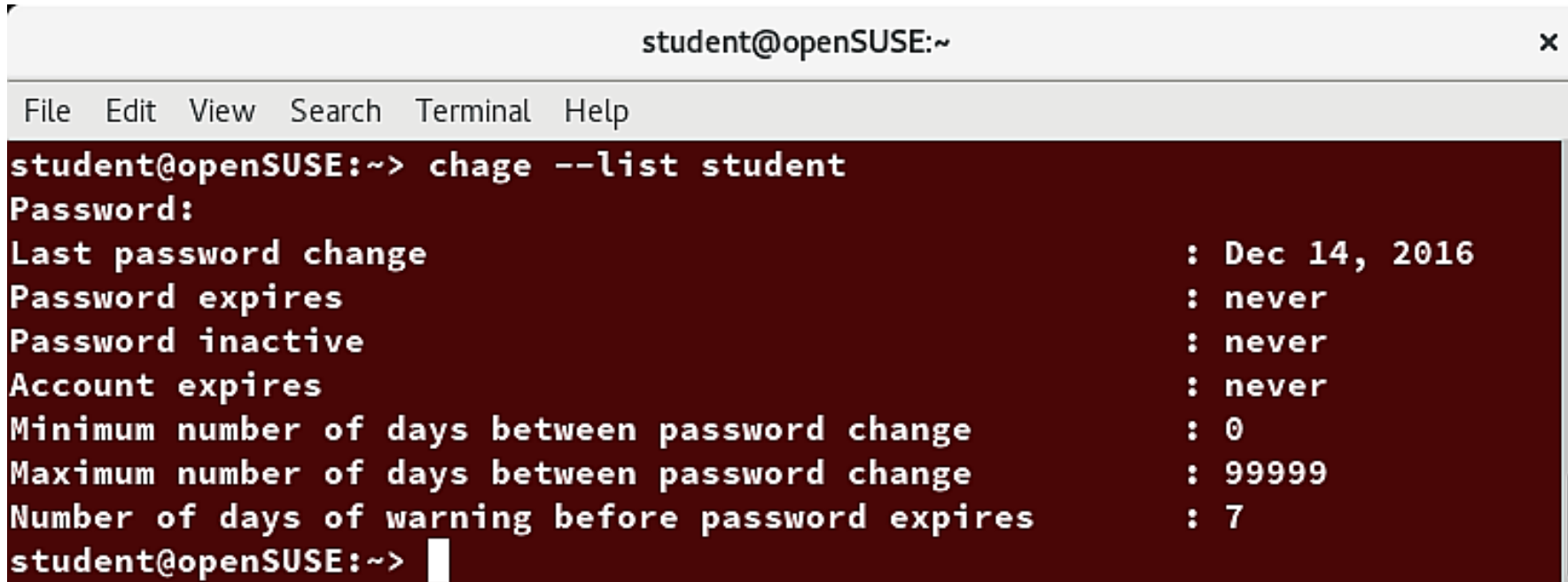
```
c7:/tmp>echo -n test | sha512sum
```

```
ee26b0dd4af7e749aa1a8ee3c10ae9923f618980772e473f8819a5d4940e0db27ac  
185f8a0e1d5f84f88bc887fd67b143732c304cc5fa9ad8e6f57f50028a8ff -
```

```
c7:/tmp>
```

Buenas prácticas con las contraseñas

Uso de contraseñas robustas y caducidad

A terminal window titled 'student@openSUSE:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the command 'chage --list student' and its output. The output lists password policy settings for the user 'student'.

```
student@openSUSE:~> chage --list student
Password:
Last password change           : Dec 14, 2016
Password expires                : never
Password inactive               : never
Account expires                 : never
Minimum number of days between password change : 0
Maximum number of days between password change  : 99999
Number of days of warning before password expires : 7
student@openSUSE:~> 
```

chage, (change age) caducidad de las contraseñas.

PAM (Pluggable Authentication Modules) obliga a los usuarios a establecer contraseñas seguras



Introducción a Linux

Trabajando con contraseñas



Introducción a Linux

Protección del proceso de arranque y los recursos hardware

Contraseña para el gestor de arranque

La contraseña **GRUB** impide que alguien cambie la configuración del arranque



La contraseña **BIOS** impedirá el arranque desde medios extraíbles

No editar directamente `/boot/grub/grub.cfg`

Editar archivos en `/etc/grub.d` y `/etc/defaults/grub`

Ejecutar `update-grub`, o `grub2-mkconfig`

Vulnerabilidades hardware

El acceso físico al hardware puede comprometer la seguridad

- Registro de teclado
- Registro de actividad en la red
- Re-montaje del disco y modificación del contenido



Política de seguridad

- Protección física de salas de servidores
- Proteger infraestructura de red
- Proteger teclados para que no sean manipulados
- Establecer contraseña de BIOS
- Cifrar el contenido de los discos

Vulnerabilidades software

Los hackers buscan y encuentran constantemente vulnerabilidades en el software



Detección de la vulnerabilidad



corrección



actualización



Introducción a Linux

Protección del proceso de arranque y los recursos hardware

```
student@centos8:/etc
[student@centos8 etc]$ tail -20 /etc/passwd
radvd:x:75:75:radvd user:/:/sbin/nologin
clevis:x:985:984:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/sbin/nologin
cockpit-ws:x:984:982:User for cockpit-ws:/:/sbin/nologin
colord:x:983:981:User for colord:/var/lib/colord:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
sssd:x:982:980:User for sssd:/:/sbin/nologin
setroubleshoot:x:981:979:/:/var/lib/setroubleshoot:/sbin/nologin
pipewire:x:980:978:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
gdm:x:42:42:/:/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:979:977:/:/run/gnome-initial-setup:/sbin/nologin
insights:x:978:976:Red Hat Insights:/var/lib/insights:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
pesign:x:977:975:Group for the pesign signing daemon:/var/run/pesign:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
student:x:1000:1000:LF Student:/home/student:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
dovecot:x:97:97:Dovecot IMAP server:/usr/libexec/dovecot:/sbin/nologin
```

Nombre de campo	Detalles	Observaciones
Nombre de usuario	Nombre de usuario de inicio de sesión	Debe tener entre 1 y 32 caracteres de longitud
Contraseña	Contraseña de usuario (o el carácter x si la contraseña se almacena en el archivo /etc/shadow) en formato cifrado	Nunca se muestra en Linux cuando se está tecleando; esto protege de las miradas indiscretas
ID de usuario (UID)	Cada usuario debe tener un identificador de usuario (UID)	<ul style="list-style-type: none">El UID 0 está reservado para el usuario rootLos UID que van del 1 al 99 están reservados para otras cuentas predefinidasLos UID de 100 a 999 están reservados para cuentas y grupos del sistemaLos usuarios normales tienen un UID de 1000 o más
ID de grupo (GID)	ID de grupo principal (GID); número de identificación de grupo almacenado en el fichero /etc/group	Se trata en detalle en el capítulo sobre <i>Procesos (Processes)</i>
Información de usuario	Este campo es opcional y permite insertar información adicional sobre el usuario, como su nombre.	Por ejemplo: Rufus T.Firefly
Directorio de inicio	Ubicación absoluta de la ruta de acceso del directorio principal del usuario	Por ejemplo: /home/rtfirefly
Shell	Ubicación absoluta del shell predeterminado de un usuario	Por ejemplo: /bin/bash