

# User Management

René Serral-Gracià<sup>1</sup>

<sup>1</sup>Universitat Politècnica de Catalunya (UPC)

February 18, 2022

# Lectures

- 1 System administration introduction
- 2 Operating System installation
- 3 **User management**
- 4 Application management
- 5 System monitoring
- 6 Filesystem Maintenance
- 7 Local services
- 8 Network services
- 9 Security and Protection
- 10 Virtualization

# Outline

- 1 Introduction
  - Goals
- 2 System Databases
- 3 User disabling and deletion
- 4 Login process
- 5 Permissions and protections

# Goals

## Coneixements

- Knowledge about the system databases
- File and Directory permissions and protections
  - SetUID/SetGID bits

## Abilities

- User management tasks
  - User creation
  - Group creation and user assignment
  - User disabling and creation

## Commands and Files

- `chmod`, `chown`, `id`, `useradd`, `userdel`, `umask`
- `/etc/passwd`, `/etc/group`, `/etc/shadow`

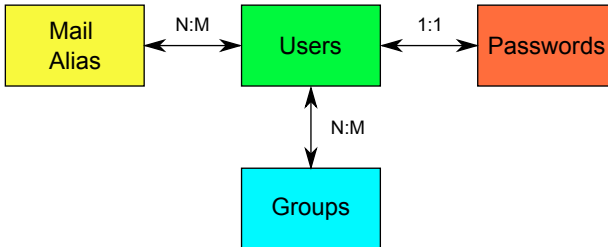
# Outline

- 1 Introduction
- 2 System Databases**
- 3 User disabling and deletion
- 4 Login process
- 5 Permissions and protections

# System Databases

per a gestió d'usuari

- /etc/passwd las contraseñas
- /etc/group \*-----\*
- /etc/shadow
- /etc/aliases



# /etc/passwd

- Must be readable by all the users

## Format

user id

username:passwd:uid:gid:real\_name:homedir:shell

group id principal

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
aramirez:x:500:500:Alex Ramirez, C6117, 54040:/home/aramirez:/bin/bash
```

usuarios de systema

*/sbin/nologin*

no te passwd

# More about users

## Specific purpose users

- root
  - UID 0 (the username does not matter)
- ftp
  - Anonymous FTP access (without password)
- www-data
  - User to run the Web Server

## System users

- Used to run services without superuser privileges
- Without shell — neither password
- Set of privileges to allow performing the tasks



# /etc/group

- A group may have lots of users
- Each user has a main group (/etc/passwd)
- Each group has a member list

## Format

groupname:passwd:gid:username,username,...

```
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
tty:x:5:
disk:x:6:root
lp:x:7:daemon,lp
mem:x:8:
kmem:x:9:
```

```
wheel:x:10:root
Mail:x:12:mail
news:x:13:news
uucp:x:14:uucp
man:x:15:
games:x:20:
ftp:x:50:
nobody:x:99:
users:x:100:aramirez
aramirez:x:500:
```

# More about groups

## Groups with special meaning — configuration dependent

- `sudo` (or `wheel`)
  - User groups with administration privileges
- `nobody`
  - Special group for NFS — used to demote privileges
- `users`
  - Normally all users belong to it
- `disk`
  - Allows users on this group to manage disks

## Purpose of groups

- Provide a neat way of easily give permissions to users
- Normally configured by the distribution – **read the manual**

# /etc/shadow

- Only accessible by root
  - Encrypted Password
  - Password expiration policy

## Format

username:passwd:password expiration policy

- passwd: change user's password
- chage: allows to change password expiration policy
  - Max/Min time between password changes
  - Account expiration date

```
root:$1$iVKd84gQ$IV7vHG0CHdIGGnYnNs00E/:12260:0:99999:7:::  
bin:*:12260:0:99999:7:::  
daemon:*:12260:0:99999:7:::  
...  
aramirez:$1$jGmk47hy$6Lkk.QYrMI67qPqvhTCdS.:12262::99999:::
```

algoritme

# /etc/aliases

- E-mail alias data base
  - Allows E-mail redirection
  - For the pseudo-users
    - to administrator
    - to programs
    - to the “outside”

```
# Basic system aliases -- these MUST be present.
mailer-daemon: postmaster
postmaster: root

# General redirections for pseudo accounts.
bin: root
webmaster: root
support: postmaster

# Person who should get root e-mail
root: aduran, xavim@ac.upc.edu
```

# Exercise

## Individually

- Detail the user creation process
  - Modification of the data bases
  - Directory creation
  - Default files
  - ...
- 0-uid, gid i decidir on estara el home  
1-/etc/passwd  
2-/etc/group  
2.5-/etc/shadow  
2.6-/etc/aliases  
3-crear home  
4-default configuration

## In group

- Gather the notes and discuss
- Make the pseudo-code for the useradd command

# User Management – Basic commands

## User Management

- `useradd (adduser) userdel`
- `usermod` — To modify all the fields except the username
- `passwd`
- `newusers` nous usuaris a punta pala
- `vipw` vi /etc/passwd

## Group Management

- `groupadd groupdel`
- `groupmod`
- `gpasswd (passwd -g)`
- `newgrp, sg` crea un sub shell amb les variables del grup
- `vigr`

# Outline

- 1 Introduction
- 2 System Databases
- 3 User disabling and deletion**
  - Disabling
  - User deletion
  - User management policies
- 4 Login process
- 5 Permissions and protections

# Disabling

## Temporarily disable an user

→ We must avoid the user access to the system

- 1 Password invalidation
  - Insert an invalid character (\*)
  - It allows to recover the original password afterward
- 2 Invalidate the shell
  - Change it with another (/bin/false, /bin/nologin)
  - Informs the user it has been disabled
  - If the user tries to login the administrator is informed

comanda chage amb nosquequin flag



# User deletion

Once we are sure the user account is not needed anymore. . .

- ❶ Disable the account (Password invalidation)
- ❷ Check that the user is not working on the system
- ❸ Backup the user's data
- ❹ Delete the user's data
- ❺ Delete the user from the system databases
  - /etc/shadow
  - /etc/passwd
  - /etc/group
- ❻ Add e-mail redirection
  - /etc/aliases

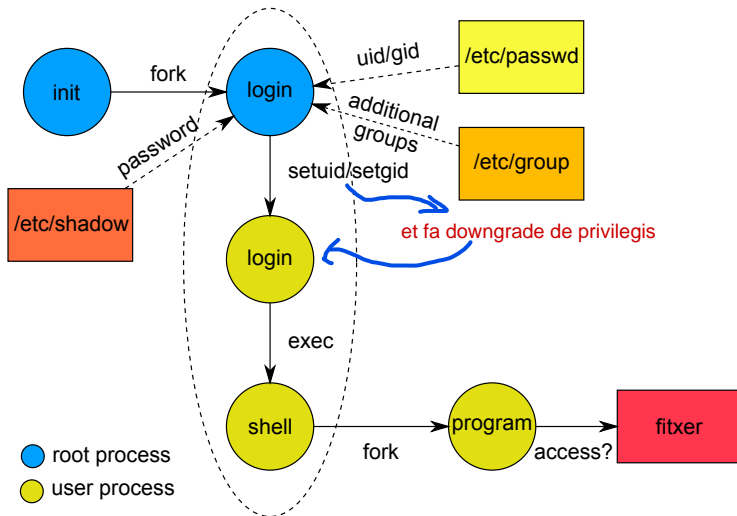
# User management policies

- **UIDs Assignment**
  - Do NOT recycle UIDs
- **username Assignment**
  - Store additional information, Office and phone number
- **Home organization** `/home`
  - Flat
    - All the users located at (`/home/...`)
  - Hierarchical, creating different directory levels
    - Based on departments... floors... offices...  
(`/home/ac/user`)
    - ... in several disks

# Outline

- 1 Introduction
- 2 System Databases
- 3 User disabling and deletion
- 4 Login process**
- 5 Permissions and protections

# Login process



# Privilege escalation

Performed through `setuid/setgid` calls

- Working as `root` is dangerous — and mostly unneeded
  - It's better to have an admin user and escalate privileges when needed
- `su [user] [-c command]`
  - Allows changing the user (by default `root`)
- `sudo [command]`
  - Allows executing a command as another user
  - Admin can restrict which commands can be executed by each user

# Outline

- 1 Introduction
- 2 System Databases
- 3 User disabling and deletion
- 4 Login process
- 5 Permissions and protections**

# Permissions and protections

(-,d) rwx rwx rwx owner group

- 3 types of permissions

- Read, write and execution (rwx)
- Regular files. . .
- Directories. . .

r->cat  
w->vi  
x->./

- 3 areas of application

- Owner, group, others (ugo)

directories perm->rwx r\_x r

- Commands:

- chown: to change a file owner
- chgrp: to change a file group
- chmod: to change permissions

r->ls  
w->mkdr  
x->cd?¿

- Set-UID/Set-GID Bits(s)



- Sticky Bit (t) only directories

mv A B --> mou el contingut de A(inode) a B (mateix sistema de fitxers, per això es tan rapid)



# Permissions and protections

	<b>Files</b>	<b>Directories</b>
r	Read the contents	List the contents
w	Write/Modify file contents	Create/Delete files
x	Run	Access the directory
SetUID	Runs with owner's UID	No effects
SetGID	Runs with owner's GID	File creation with the same group as the directory owner
Sticky Bit	No effects	Only the file owners can erase them



## Exercise – In group

- Assign the directory and file protections for the file. . .

```
$ ls -l ./dirdades/dades.txt  
-rw-rw-r-- 1 aso01 aso01 9778 Nov 28 18:10 ./dirdades/dades.txt
```

- Can only be modified by the owner
- Readable only by its group
- Only deletable by its owner
- Only the owner can run “ls” in the directory

## Exercise – In group

- Assign the directory and file protections for the file. . .

```
$ ls -l ./dirdades/dades.txt  
-rw-rw-r-- 1 aso01 aso01 9778 Nov 28 18:10 ./dirdades/dades.txt
```

- Can only be modified by the owner
  - `-w-`   `---`   `---`
- Readable only by its group
  - `---`   `r--`   `---`   + `dir`   `---`   `--x`   `---`
- Only deletable by its owner
  - `dir` → `-w-`   `---`   `---`
- Only the owner can run “ls” in the directory
  - `dir` → `rw-`   `---`   `---`

```
$ ls -la ./dirdades/dades.txt  
drwx--x--- 1 aso01 aso01 1024 Nov 28 18:11 .  
-rw-r----- 1 aso01 aso01 9778 Nov 28 18:11 ./dirdades/dades.txt
```

# Default permissions

## During file/directory creation...

- Owner is determined by current user and group
  - `id` informs about current user/group
  - `newgrp` allows changing the current group
- Permissions are determined by `umask`: user mask
  - Indicates which permissions **DO NOT** belong by default to the file or directory

```
022: rwx r-x r-x
027: rwx r-x ---
```

# Homework

## Application installation mechanisms

- Software distribution formats
  - tar, gz, rpm, deb, zip. . .