# Linux Administration

## Users and groups

Xavier Belanger

# Users and groups

- One specific account exists to manage the system: root [1].
- All other accounts are users; some are for regular end-users, some are service accounts for applications.
- Users can be grouped by groups, every user is at least member of a group.

1: Ubuntu is a notable exception

# The root account

- This account has full privileges and full access to the system.
- No permission checks are made when using the root account.
- Usage of the root account should be limited to the strict minimum; regular system administration tasks should be performed using sudo.

# Users and groups information

- User accounts basic information is stored in the */etc/passwd* file.
- Except for the password hash, stored in */etc/shadow* along with expiration dates.
- Groups information is stored in the */etc/group* file.

# /etc/passwd structure

The /etc/passwd file contains 7 fields, separated by colons:

- username
- ‘x’ for the encrypted password
- user ID
- group ID
- name and description
- home directory
- shell

# /etc/shadow structure

The /etc/shadow file contains 9 fields, separated by colons:

- username
- encrypted password
- date of last password change
- minimum password age
- maximum password age
- password warning period
- password inactivity period
- account expiration date
- reserved field for future use

# /etc/group structure

The /etc/group file contains 4 fields, separated by colons:

- group name
- password
- group ID
- user list, comma separated

# User and group tools - 1

- *adduser*, *useradd*, *usermod*, *userdel*, *newusers*: to add, remove and modify user accounts
- *groupadd*, *groupdel*, *groupmod*: to add, remove and modify groups
- *vipw*, *vigr*, *pwck*, *grpck*: to manipulate and verify user and group files

# User and group tools - 2

- *whoami*, *id*, *logname*, *groups*: used to identify a user account and groups
- *chfn*, *chsh*, *chage*: used to modify a user account
- *passwd*: used to modify a password

# Using sudo

- *sudo* is a tool that can provide limited administrative access to regular users.
- The principle is to list only authorized commands for a specific user (or a group), then the user will need to enter their own password before running one of those commands.

# Configuring sudo

- The */etc/sudoers* file contains the configuration for sudo (allowed users and groups, commands, …).
- The /etc/sudoers file should be edited with the *visudo* command to avoid syntax errors and other protections.

# The su command

- This command allows to impersonate (“switch”) entirely to another user account, if authorized.
- *su* should be used with caution, and for a good reason, usually for troubleshooting.