GNU/Linux Course

May 18th 2011

Puria Nafisi Azizi (puria) puria@netstudent.polito.it

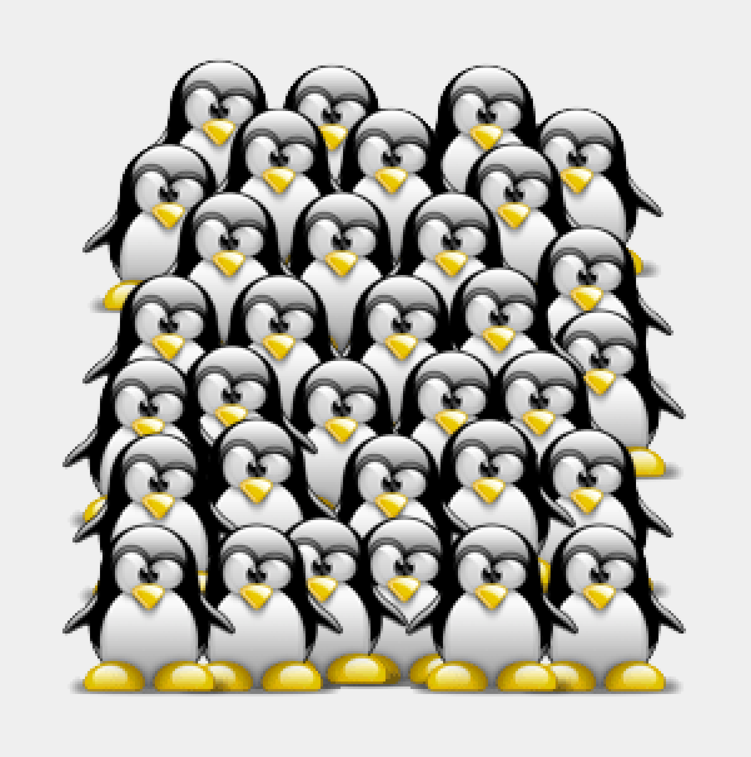
http://netstudent.polito.it

User management

Where to dare passwords

Of laziness and immobility

Permits



User management

Unix has permission from the earliest versions, for different users to work simultaneously on the system, as well as GNU / Linux is a multiuser system, so the permissions and restrictions on individual users and groups are much more stringent than on other proprietary systems for as households and very similar to what is coded for enterprise-class systems.

In summary, a user's data can not be edited and viewed by other users except in the case that this is explicitly permitted (obviously the root user has no limitations).

User management

Even the operations you can perform on a GNU / Linux are subject to this permit system, which effectively makes it even more difficult the creation and spread of viruses on GNU / Linux.

To access a GNU / Linux, except in rare cases, you must log into the system by entering your username and password.

User management

adduser / useradd: When invoked without the **-D** option, the **useradd** command creates a new user account using the values specified on the command line and defaults by the system. The new user account is added to the system files that need it, you will create the home directory, and there you will copy the original file, depending on the options on the command line.

The main options that apply to the **useradd** command are

-d home_dir

The new user is created using home_dir as the value for the user's login directory.

User management

-e expiration_date

The time off dell"account user (MM / DD / YY).

-f giorni_inattività

The number of days after password expires until the account is permanently disabled. 0 disables the account immediately, -1 to disable this feature.

-g gruppo_iniziale

User group name or GID, which must exist.

User management

follows **adduser / useradd**

-G group,[...]

Other groups the user belongs. Must be entered separated by commas, no spaces.

-s shell

The name of the user's login shell.

User management

-u uid

The numerical value of the user. This value must be unique, unless you used the **-o** option. The value must be non-negative. The default behavior is to use the smallest ID value greater than 999 and greater than that of any other person. Values between 0 and 999 are typically reserved for system accounts.

File Reference:

/etc/passwd - user account information

/etc/default/useradd - default information

/etc/skel - directory containing default files

User management

*With the **-D** option, useradd displays the current default values, and you can change these parameters*

***-b** home_predefinita*

The path prefix for the new user's home directory. The user name will be added at the end of home_predefinita to create the new directory name.

***-e** data_scadenza_predefinita*

Date of disabling the user account.

User management

-f inattività_predefinita

Number of days after the expiry pwd before disabling account.

***-g** gruppo_predefinito*

The name or ID of the initial group for a new user.

***-s** shell_predifinita*

The name of the login shell for new user

*Without options, **useradd** displays the default values.*

User management

chsh: *Allows you to change the user's shell*

chsh [-s shell] [-l] [username]

the only valid shells are those listed in the file **/etc/shells**

Options:-s, - shell-l, - list-shells

User management

***Usermod**: This command lets you change a user's account*

Options:

-c comment: The comment field of the new user's password file.

-d home_dir: new login directory. With the-m option is traversed the content current home.

-e expiration_date: the date of disabling user.

-f giorni_inattività: days of inactivity before disabling the account.

User management

passwd: *Modify the login password of a user*

passwd [user [password]]

The new password must be at least six characters long and can consist of both uppercase and lowercase letters or non-alphabetic characters. Obviously you can not use your name as a password.

When using the command by root, the rules for passwords are not enforced and does not require the old password in advance.

gpasswd: to enter the password for the administrative groups and the **/etc/group** and possibly **/etc/gshadow**

User management

Syntax:

gpasswd group

gpasswd -a user group

gpasswd -d user group

gpasswd -R group

gpasswd -r group

gpasswd [-A user,...] [-M user,...] group

User management

groupadd: - Create a new group

groupadd [-g gid [-o]] group

-g *gid*

numeric identifier (ID) of the group. Values between 0 and 99 are typically reserved for system accounts.

User management

groupdel: *- Deletes a new group*

groupdel group

You can not delete primary group of existing users, the command does not alter in any way the existing GID of files that must be changed manually.

newgrp: - logs into a new group: This command allows to change the GID of a user. A necessary condition is that the user belongs to the group whose GID want.

User Management

Where to dare passwords

Of laziness and immobility

Permits

… le password

/etc/passwd contains the entire database of users of the system, enclosed in a plain text file. It is sometimes also referred to as the password file, although in practice, with the introduction of / etc / shadow file that no longer contains the password.

1. Username.

2. Password in encrypted form, or in the presence of x / etc / shadow.

3. Numeric user ID.

4. Group ID number.

5. Full name or description of account.

6. Home directory.

7. Login shell.

… le password

The file **/etc/passwd** is readable by all users of the system, so that the search for someone else, but this also means that a system with no **/etc/shadow** in this file also contains the password, even in encrypted form.

… le password

/etc/group contains all the groups database enabled on the system in the form of text files and has a very simple structure of the record:

Group: password: GID: user list

group

This is the name that identifies the group, along with its GID.

password

If used, the group password in this file is stored in encrypted form, and there are any restrictions for this file in / etc / passwd. The use of group passwords is not very widespread.

… le password

GID

It is the identification number of the group is the value entered in /etc/passwd to specify the default group of a user. A user can belong to several distinct groups of course, but can have only one default group.

user list

The set of all users in a group.

… le password

Unfortunately, the encrypted passwords in / etc / passwd, especially in the presence of weak passwords, or without reasonable safety criteria (too short or trivial) can be decoded in a short time with modern systems.

From here the need to store passwords in another file, /etc/shadow, in fact, only readable by root and in which passwords are still stored in encrypted form: no administrator should be able to know user passwords.

For added security, finally, only the authentication programs and management may have access to **/etc/shadow**, that looks like this:

username:password:lastchange:min:max:warn:inactive:expire:

… le password

username: user name.

password: encrypted password or * (user disabled) and! (no password).

lastchange: number of days since last password change (in a Unix, so from January 1, 1970).

min: minimum days before they can change the password.

max: maximum password age (always in days);

warn: number of days notice for the password.

inactive: the number of days of inactivity the user is granted

expire: Date of disabling the account.

… le password

It's important to remember that normally the idle and the "due date" are not set by default with the standard commands of the users configuration.

User Management

Where to dare passwords

Of laziness and immobility

Permits

Della pigrizia...

The use of the shell allows to work remotely, or through the network as if you were acting locally.

In reality, the remote access is much more aware of what you do not believe in the use of systems: it is typical that the servers are located in designated areas that are not normally accessible and administered remotely.

The most common method to access these machines was the telnet: This term means either the terminal program that the communication protocol.

Della pigrizia...

Telnet is used to establish connections with remote systems and use the shell, but has a big problem of security: **username and password are transmitted without encryption** and are therefore easily identifiable.

That's why you created the **SSH** protocol which provides for the use of an encrypted connection for authentication procedures and management.

User Management

Where to dare passwords

Of laziness and immobility

Permits

Permessi

All files, directories, links, etc. feature permits

The permissions (or ACL) are attributes that restrict user access to files

They are based on identifying the user and user groups, and setting at least read, write and execute

Permessi

Each user accessing the system is characterized by a number uid

This number may not be unique

In addition, each user belongs to one or more groups, indicated by the number gid

Root usually has uid 0

Each file belongs to a user and a group

Permessi

Read permission (r) indicates the read-only access the contents of the file

The write permission (w) allows editing and deleting the file

The permission to execute (x) allows the execution of a file

All programs (including the basic commands visas) are permitted to run

Execute permission on a directory means the possibility of access (eg with 'cd Nomeda')

Permessi

The executable is therefore not possible with the extension but the 'x'

Permits r, w, x, and the user group of a file can be viewed with 'ls-l'

The first group consists of 10 characters:

A character indicating the type of file, which can not be changed (is decided at creation)

'-' indicates normal file, 'd' directory, 'l' Link, 's' socket ...

Permessi

Three groups of three characters of the form 'rwx'

The first group refers to the permission of the owner (u - user)

The second group indicates the permissions of the group (g-group)

The third group indicates the permissions of other users and groups (or-others)

If the letter of permission is present, the privilege is granted, otherwise this is a '- '

Permessi

This is followed by an indication of the file owner, size, and the creation time

For example, the string '-rw-r - r -' indicates a normal file that can be read by and written only by the owner

A directory with read permission but not execute ('drw-rw-rw-') allows anyone to list and edit the files, but does not allow access (for example with 'cd')

Permessi

The permissions and ownership can be modified with three basic commands

'FILENAME USERNAME chown'is used to change the owner of a file

Only root can arbitrarily set the properties file

A normal user can not "give" his file to another user

'chgrp GROUPNAME FILENAME'is used to set the file's group

Permessi

'chmod'is used to change the sequence of permissions on a file

`It has two modes of use

Through explicit indication of permits r, w, x to the utilities u, g, or

It is possible to assign, add or remove permissions for the user or group

Example 'chmod go-w FILENAME'

If the audience is not specified, includes all three (eg 'chmod + rw FILENAME')

Permessi

To accurately assign permissions 'chmod u = rw, go = r FILENAME'

`The second mode is to represent the triad of 8 rwx numbers:

--- = 0, 1 = - x, 2 =-w-3 =-wx, 4 = r -, 5 = rx, 6 = rw-, 7 = rwx

Set 'chmod 777 FILENAME' is therefore equivalent to allow any work at all ('rwxrwxrwx')

Permessi

It is then this is a program that handles the default permissions when you create a file. 'umask' with no arguments shows the form currently used

The mask is in numeric format of chmod, but reversed

For example, 022 indicates that a directory will be created with permissions 755 ', or' rwxr-xr-x '

The normal files, which are not executable by default, are usually deprived of 'x'

Copyleft

Copyleft

Quest'opera, per volontà degli autori, è rilasciata sotto la disciplina della seguente licenza

Creative Commons Public License

Attribuzione-Condividi allo stesso modo 2.5 Italia

Tu sei libero:

di riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare quest'opera

di modificare quest'opera

Alle seguenti condizioni:

Attribuzione. Devi attribuire la paternità dell'opera nei modi indicati dall'autore o da chi ti ha dato l'opera in licenza e in modo tale da non suggerire che essi avallino te o il modo in cui tu usi l'opera.

Condividi allo stesso modo. Se alteri o trasformi quest'opera, o se la usi per crearne un'altra, puoi distribuire l'opera risultante solo con una licenza identica o equivalente a questa.

Ogni volta che usi o distribuisci quest'opera, devi farlo secondo i termini di questa licenza, che va comunicata con chiarezza. In ogni caso, puoi concordare col titolare dei diritti utilizzi di quest'opera non consentiti da questa licenza. Questa licenza lascia impregiudicati i diritti morali. Le utilizzazioni consentite dalla legge sul diritto d'autore e gli altri diritti non sono in alcun modo limitati da quanto sopra.

Questo è un riassunto in linguaggio accessibile a tutti del codice legale (la licenza integrale) che è disponibile alla pagina web:

http://creativecommons.org/licenses/by-sa/2.5/it/legalcode

Copyleft

Quest'opera, è stata realizzata grazie al contributo di molte persone. La prima versione è stata realizzata a partire dalle slide realizzate da Silvio Colloca distribuite con licenza Creative Commons sul sito http://linuxhelp.it. Successivamente sono state modificate dai molti docenti che hanno prestato il loro servizio gratuito nelle lezioni dei corsi Netstudent. In ordine sparso (e sperando di non dimenticare nessuno): Giovanni Berton Giachetti, Daniele Lussana, Alessandro Ugo, Emmanuel Richiardone, Andrea Garzena, Stefano Cotta Ramusino, Roberto Preziusi, Marco Papa Manzillo, Puria Nafisi Azizi, Luca Necchi, Luca Barbato, David Putzer, Alberto Grimaldi, Nicola Tuveri, Stefano Colazzo, Laura De Martini, Luca Bruno, ecc...