Operating System II

Malak Chniter

maleek.chniter@ieee.org

Google Classroom:
Joining Instructions

1. Access Google Classroom using your **Gmail** account;

2. Click on the **'Join'** button;

3. Enter the class code: **uswy3qp** ;

4. Click **'Join Class'** to become a member;

Plan

Chapter I: Linux – Users and Access Permissions

1. Introduction
2. Types of User Accounts on Linux
3. Managing Users
4. Managing Groups
5. Permissions
6. Exercises

1. Introduction

- Linux System is typically used by **Multiple Users;**

- Each User has an **Identifier (login)**, **password, Unique User Identifier**, **Group Identifier**, **User-info**, **Home Directory**, **Shell**

- Linux System allows **users** to **use files** while **limiting the access permissions for each** to ensure the integrity of their data.

- For organizational purposes, **users** will be **classified** into different **groups**.
	E.g Std1:1st-Year GLSI

1. Introduction

Try this command >>~$ **cat /etc/passwd**

The file /etc/passwd contains information about all users of the system. Each line in the file pertains to one user

Login: the identifier that the user must enter to authenticate themselves

User Identifier (UID): Unique identifier of the user, in the form of a numerical value.
The root user has the UID 0. UIDs>100 are used for system accounts

Group Identifier (GID): Identifier of the user's group

Home directory: directory where files belonging to the user are stored. Typically in the form "/home/user".

```
malak@malak-VirtualBox:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nolog
in
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr
/sbin/nologin
```

Password: crypted password. It has different significations:
*: It is impossible to authenticate on the system with this account;
!!: The account is disabled;
x or ! : The password is in a shadow file;
Empty field: There is no password for this account.

User-info: full name and other information such as the phone number... Each piece of information is separated by a comma ","

Shell: indicates which command interpreter will be launched after authentication

1. Introduction

Try this command >>~$ **cat /etc/group**
This file contains information about the groups present on the system.

Name: name of group

*: linked to older versions of Unix. It is no longer used and may remain empty or contain the characters * or x.

GID: Unique identifier of the group in the form of a numerical value.

User(s): This is the list of users belonging to the group. The different users are separated by commas..

```
malak@malak-VirtualBox:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,malak
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:malak
floppy:x:25:
tape:x:26:
sudo:x:27:malak
audio:x:29:pulse
```

1. Introduction

Try this command >>~$ **cat /etc/shadow**   **what happened!?**
passwords are stored in this file, <u>which can only be read by the administrator</u>

>>~$ **sudo cat /etc/shadow**

```
malak@malak-VirtualBox:~$ sudo cat /etc/shadow
root:!:19379:0:99999:7:::
daemon:*:17647:0:99999:7:::
bin:*:17647:0:99999:7:::
sys:*:17647:0:99999:7:::
sync:*:17647:0:99999:7:::
games:*:17647:0:99999:7:::
man:*:17647:0:99999:7:::
lp:*:17647:0:99999:7:::
mail:*:17647:0:99999:7:::
news:*:17647:0:99999:7:::
uucp:*:17647:0:99999:7:::
proxy:*:17647:0:99999:7:::
www-data:*:17647:0:99999:7:::
backup:*:17647:0:99999:7:::
list:*:17647:0:99999:7:::
irc:*:17647:0:99999:7:::
gnats:*:17647:0:99999:7:::
nobody:*:17647:0:99999:7:::
systemd-network:*:17647:0:99999:7:::
systemd-resolve:*:17647:0:99999:7:::
syslog:*:17647:0:99999:7:::
messagebus:*:17647:0:99999:7:::
apt:*:17647:0:99999:7:::
```

2. Types of User Accounts on Linux

1. We can distinguish three types of accounts:

- **Root administration account**: The root account is the superuser account that has full control over the system. It has unrestricted access to all files and commands and can perform any operation. This account is typically used for system administration tasks and making system-wide changes.

- **Application accounts**: These accounts are used by specific applications or services running on the system. They are often created during the installation of software and are used exclusively by those applications to run their processes.

- **Regular user accounts**: These accounts are created for individual users who interact with the system on a regular basis. They have limited privileges and can only perform certain operations on files and directories that they own or have permission to access. Regular user accounts are used for everyday tasks and do not have administrative privileges.

```
malak@malak-VirtualBox:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nolog
in
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr
/sbin/nologin

malak:x:1000:1000:malak,,,:/home/malak:/bin/bash
```

3. Managing Users

a. Add a User

Command syntax >>~$ useradd options login

E.g : Try>>~$ **useradd YourName**

To know the different existing options >>~$ **useradd –help**

This command is used to display or modify default useradd configuration settings. When you use "useradd -D", it shows the current default settings for creating new user accounts. You can also use additional options with "useradd -D" to modify these default settings. For example, "useradd -D -s /bin/bash" would set the default shell for new user accounts to "/bin/bash".

```
malak@malak-VirtualBox:~$ useradd -help
Usage: useradd [options] LOGIN
       useradd -D
       useradd -D [options]

Options:
  -b, --base-dir BASE_DIR       base directory for the home directory of the
                                new account
  -c, --comment COMMENT         GECOS field of the new account
  -d, --home-dir HOME_DIR       home directory of the new account
  -D, --defaults                print or change default useradd configuration
  -e, --expiredate EXPIRE_DATE  expiration date of the new account
  -f, --inactive INACTIVE       password inactivity period of the new account
  -g, --gid GROUP               name or ID of the primary group of the new
                                account
  -G, --groups GROUPS           list of supplementary groups of the new
                                account
  -h, --help                    display this help message and exit
  -k, --skel SKEL_DIR           use this alternative skeleton directory
  -K, --key KEY=VALUE           override /etc/login.defs defaults
  -l, --no-log-init             do not add the user to the lastlog and
                                faillog databases
  -m, --create-home             create the user's home directory
```

```
  -M, --no-create-home          do not create the user's home directory
  -N, --no-user-group           do not create a group with the same name as
                                the user
  -o, --non-unique              allow to create users with duplicate
                                (non-unique) UID
  -p, --password PASSWORD       encrypted password of the new account
  -r, --system                  create a system account
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --shell SHELL             login shell of the new account
  -u, --uid UID                 user ID of the new account
  -U, --user-group              create a group with the same name as the user
  -Z, --selinux-user SEUSER     use a specific SEUSER for the SELinux user mappi
ng
      --extrausers              Use the extra users database
```

3. Managing Users

b. Delete a User

Command syntax >>~$ userdel options login

E.g : Try>>~$ **userdel YourName**

To know the different existing options >>~$ **userdel –help**

```
malak@malak-VirtualBox:~$ sudo userdel user2
malak@malak-VirtualBox:~$ userdel -help
Usage: userdel [options] LOGIN

Options:
  -f, --force                    force removal of files,
                                 even if not owned by user
  -h, --help                     display this help message and exit
  -r, --remove                   remove home directory and mail spool
  -R, --root CHROOT_DIR          directory to chroot into
      --extrausers               Use the extra users database
  -Z, --selinux-user             remove any SELinux user mapping for the user
```

3. Managing Users

c. Modify a User account

Command syntax >>~$ usermod options login

E.g : Try>>~$ **userdmod -d /home/YourName –m user2**

> **->** change user2's home directory to /home/YourName. This command also copies the contents of the old home directory and adjusts the permissions.

<u>To know the different existing options</u> >>~$ **usermod –help**

```
File  Edit  View  Search  Terminal  Help
malak@malak-VirtualBox:~$ sudo usermod -d /home/user2 -m user1
malak@malak-VirtualBox:~$ usermod -help
Usage: usermod [options] LOGIN

Options:
  -c, --comment COMMENT         new value of the GECOS field
  -d, --home HOME_DIR           new home directory for the user account
  -e, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -g, --gid GROUP               force use GROUP as new primary group
  -G, --groups GROUPS           new list of supplementary GROUPS
  -a, --append                  append the user to the supplemental GROUPS
                                mentioned by the -G option without removing
                                him/her from other groups
  -h, --help                    display this help message and exit
  -l, --login NEW_LOGIN         new value of the login name
  -L, --lock                    lock the user account
  -m, --move-home               move contents of the home directory to the
                                new location (use only with -d)
  -o, --non-unique              allow using duplicate (non-unique) UID
  -p, --password PASSWORD       use encrypted password for the new password
  -R, --root CHROOT_DIR         directory to chroot into
```

```
  -s, --shell SHELL             new login shell for the user account
  -U, --uid UID                 new UID for the user account
  -U, --unlock                  unlock the user account
  -v, --add-subuids FIRST-LAST  add range of subordinate uids
  -V, --del-subuids FIRST-LAST  remove range of subordinate uids
  -w, --add-subgids FIRST-LAST  add range of subordinate gids
  -W, --del-subgids FIRST-LAST  remove range of subordinate gids
  -Z, --selinux-user SEUSER     new SELinux user mapping for the user account
malak@malak-VirtualBox:~$
```

3. Managing Users

d. Manage the password of a user

Command syntax >>~$ passwd options login

E.g : Try>>~$ **passwd YourName**

To know the different existing options >>~$ **passwd –help**

```
malak@malak-VirtualBox:~$ passwd -help
Usage: passwd [options] [LOGIN]

Options:
  -a, --all                      report password status on all accounts
  -d, --delete                   delete the password for the named account
  -e, --expire                   force expire the password for the named account
  -h, --help                     display this help message and exit
  -k, --keep-tokens              change password only if expired
  -i, --inactive INACTIVE        set password inactive after expiration
                                 to INACTIVE
  -l, --lock                     lock the password of the named account
  -n, --mindays MIN_DAYS         set minimum number of days before password
                                 change to MIN_DAYS
  -q, --quiet                    quiet mode
  -r, --repository REPOSITORY    change password in REPOSITORY repository
  -R, --root CHROOT_DIR          directory to chroot into
  -S, --status                   report password status on the named account
  -u, --unlock                   unlock the password of the named account
  -w, --warndays WARN_DAYS       set expiration warning days to WARN_DAYS
  -x, --maxdays MAX_DAYS         set maximum number of days before password
                                 change to MAX_DAYS
```

3. Managing Users

e. Display information about a user

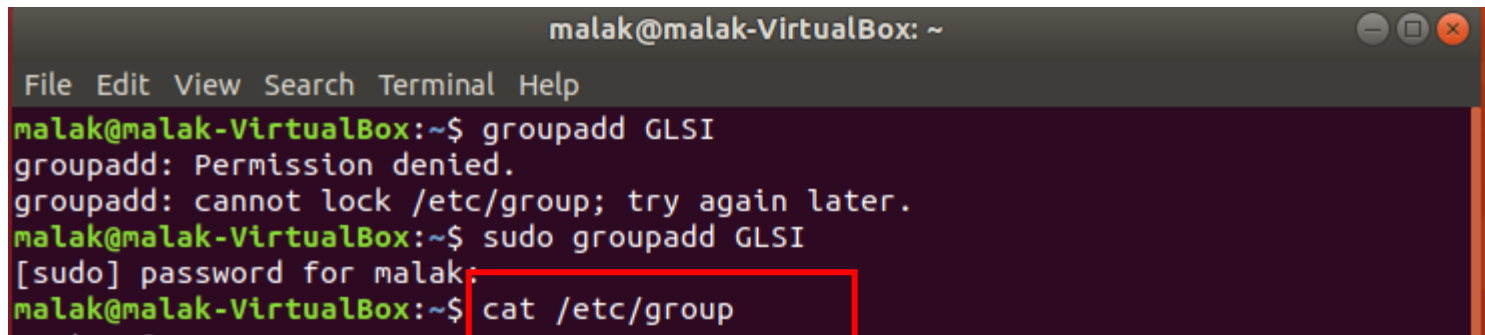Commands syntax >>~$ whoami , w , who or users

E.g : Try>>~$ whoami , w , who and users

4.   Managing Groups

a.   Create a group

Commands syntax >>~$ groupadd option groupName

E.g : Try>>~$ **groupadd GLSI1**

To verify

5. Managing Groups

a. add a group

To know the different existing options >>~$ **groupadd –help**

```
malak@malak-VirtualBox:~$ groupadd -help
Usage: groupadd [options] GROUP

Options:
  -f, --force                   exit successfully if the group already exists,
                                and cancel -g if the GID is already used
  -g, --gid GID                 use GID for the new group
  -h, --help                    display this help message and exit
  -K, --key KEY=VALUE           override /etc/login.defs defaults
  -o, --non-unique              allow to create groups with duplicate
                                (non-unique) GID
  -p, --password PASSWORD       use this encrypted password for the new group
  -r, --system                  create a system account
  -R, --root CHROOT_DIR         directory to chroot into
      --extrausers              Use the extra users database
```

5. Managing Groups

a. **add a group (to users)**

Command Syntax>>~$ useradd –g GroupName UserName

-> to add a user to a specific group

```
malak@malak-VirtualBox:~$ sudo useradd -g newMe malak2
[sudo] password for malak:
```

Command Syntax>>~$ useradd –g GroupName –G SecondaryGroupName UserName

-> to add a user to a SECONDARY group

=> Groups should be created before adding users to them

5. Managing Groups

b.   Modify a group

Commands syntax >>~$ groupmod –n Newgroup Oldgroup

E.g : Try>>~$ **groupmod –n GLSI_official GLSI1**

```
malak@malak-VirtualBox:~$ sudo groupmod -n newMe MeMe
malak@malak-VirtualBox:~$ cat /etc/group
```

To know the different existing options >>~$ **what to do???**

5. Managing Groups

b. Delete a group

Commands syntax >>~$ groupdel groupName

E.g : Try>>~$ **groupdel GLSI1**

```
malak@malak-VirtualBox:~$ sudo groupdel GLSI
malak@malak-VirtualBox:~$ cat /etc/group
```

To know the different existing options >>~$ **groupdel –help**

```
malak@malak-VirtualBox:~$ groupdel -help
Usage: groupdel [options] GROUP

Options:
  -h, --help                      display this help message and exit
  -R, --root CHROOT_DIR           directory to chroot into
  -f, --force                     delete group even if it is the primary group of
 a user

malak@malak-VirtualBox:~$
```

5. Managing Groups

c. Display groups

To find out which groups a user belongs to, use the command "groups".

➔ If you do not specify a user name, these are the groups of the current user which will be displayed.

To find out the groups of a particular user, simply enter their login in command argument

```
malak@malak-VirtualBox:~$ groups malak3
malak3 : newMe newMe2
malak@malak-VirtualBox:~$
```

5. Permissions

a. The different users of a file

File ownership refers to which user owns the file, who owns it. From this possession (or not), it will then be possible to set access permissions on the file. Access permissions on the file are set by the owner of the file Three categories of users of a file:

1. The user of the file (**u**): This is the creator of the file;
2. The group of the file (**g**). The user is in the same group as the creator of a file;
3. the others (**o**). Neither the owner of the file nor a member of the same group as the owner of the file.

5.   Permissions

b. The permissions

Any user (**u**, **g**, or **o**) can have read and write access to a file, and has no access to another file, for example.

Three Types of permissions:

1. Reading (r): allows you to access the contents of a file: listen to an audio track, watch a movie, read a text, list the contents (ls) of a directory.
2. Writing (w): allows you to create and edit a file (correct text and make updates), rename or delete a file in a folder; etc.)
3. Running/excute (x): allows you to: Execute programs (software), change to the current directory (cd).

5. Permissions

- Every user (u, g or o) has 3 permissions:
    - Try this command>> ~$ **ls -l**
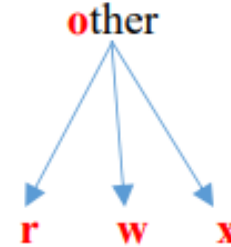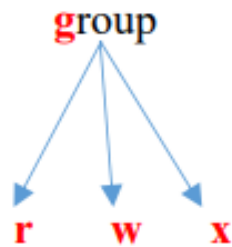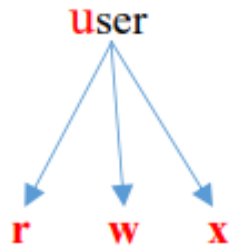
5. Permissions

c. "chmod" Command

-> "change mode" Allows you to change permissions on a file. The chmod command can be used in two ways:

1. either by specifying permissions in an octal way (which we will see later);
2. by adding or removing permissions to one or more categories of users using the symbols r, w and x.

HOW???

5. Permissions

The allocation of rights is done separately. In this way, we will choose:

1. To whom does the change apply?

    u (user) represents the "owner" category;

    g (group) represents the category "owning group";

    o (others) represents the "rest of the world" category;

    a (**all**) represents all three categories.

2. The change you want to make

    + : add

    - : delete

    - = : assignment

3. The right you want to change

    r : read ⇒ read;

    w : write ⇒ write

    x : execute ⇒ execution

6. Exercises

- **App 1)°:**
  a. Place yourself under the **root** directory, then specify the access rights of each file/directory located under the root.
  b. Create a new group using the **groupadd** command with the name of your group (example: GLSI_ESPIN). Verify that the created group is added to the list of groups.
  c. Create two users, Student1 and Student2, who belong to the previously created group (as their primary group). The user account Student1 must be created in /home and the user account Student2 must be created in /home/web.
  d. Assign a password for each of the two created users.

6. Exercises

- **App 2)°: (App 1 continued)**
  a. Create a group "**ESPIN_University**".
  b. Modify the user account Student2 to have **ESPIN_University** as its secondary group.
  c. Add a user **Teacher** with **ESPIN_University** as the primary group and belonging to a secondary group **Teachers**.
  d. Using the groups command, verify which group each user belongs to.
  e. Log in with the Student1 account and create the following directory structure.

/

home

Applications-OS

Rep1

Rep2

Rep3
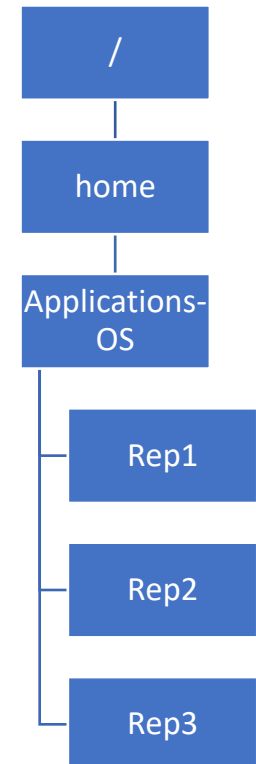
6. Exercises

- **App 3)°: (App 1 continued)**
  a. What are the default permissions of the folders in this directory tree?
  b. Grant full access permissions to the **Applications_OS** directory and all its subdirectories for all users.
  c. Create a new file named "**F1.txt**" in the **Applications_OS** directory by writing some lines in this file. What are the default access rights granted to this file?
  d. Modify the permissions of the "**F1.txt**" file to **r-- r-- r--** (mention two different methods). Verify that the new access rights are effective by attempting to edit the file.
  e. Create a file named "**Script.sh**" in the **Applications_OS** directory and grant it the following permissions **rwx r-- r--**. How can you verify that the group and others permissions are effective?
  f. Delete the Teachers group. Verify if it has been successfully deleted.
  g. Delete the user Student2 as well as their home directory.

Corrections

- **App 1)°:**

  a. Tap: cd /
      ls –l

  b. sudo groupadd GLSI_ESPIN

  cat /etc/group

  c. sudo adduser Student1

  sudo usermod –g GLSI_ESPIN Student1

  sudo adduser Student2

  sudo usermod –g GLSI_ESPIN Etudiant2 –d /home/web

  d. sudo passwd Student1
  sudo passwd Student2

Notes

- The -g argument specifies the primary group to which the user belongs, and the -G argument specifies the secondary group (if necessary).

- If a user is created without specifying the group, then the Linux system creates a group with the same name as that user (this is the primary group of the user in question).

- To check the list of existing user accounts: cat /etc/passwd"

Corrections

- **App 2)°: (App 1 continued)**
  a. Tap: sudo groupadd ESPIN_University
  b. sudo usermod –G ESPIN_University Student2
  c. sudo useradd –g ISIMS –G Teachers Teacher
  d. groups Student1
     groups Student2
     groups Teacher
  e. su Student1
  f. ls -l

Corrections

- **App 3)°: (App 1 continued)**
  - a. ls -l
  - b. chmod o+w Applications_OS
    cd Applications_OS
    chmod o+w Rep1
    chmod o+w Rep2
    chmod o+w Rep3
  - c. gedit F1.txt
    default access permissions are: rw (user), rw (group), r (other)
  - d. Method 1 (symbolic): chmod u-w,g-w F1.txt
    Method 2 (octal): chmod 444 F1.txt.
    r => 4
    w => 2
    x => 1
  - e. gedit Script.sh
    chmod 644 Script.sh
  - f. groupdel Enseignants
    cat /etc/group (to verify)
  - g. userdel –r Student2

Plan

Chapter 2: Linux – Shell programming Part I

1. Introduction
2. Kernel definition
3. Shell definition
4. Difference between Line Shell and Graphical Shell
5. Basic Shell commands
6. Exercises