ADS Lab 07 - Account Management

Authors: Vincent Peer, Pablo Urizar

Date: June the 4th, 2023

Task 0: Examine the setup of your own account

> Examine your account by using the command id and by looking into the files /etc/passwd and /etc/group . What is its principal group? What other groups is the account a member of? What is the UID of the account and the GID of the principal group?

```
$ id
uid=1000(vpeer) gid=1000(vpeer)
groups=1000(vpeer),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(d
ip),44(video),46(plugdev),116(netdev),1001(proj_a),1002(proj_b)
```

- The principal group is vpeer
- The account is also member of the following groups : adm, dialout, cdrom, floppy, [...], proj_a, proj_b
- The UID is 1000 and de GID of the principal group is also 1000

> Which skeleton files have been copied?

Files in /etc/skel, so .bash_logout, .bashrc and .profile.

Task 1: Create user accounts

1. Create the groups jedi and rebels . Before creating them verify that they do not yet exist.

```
$ grep -e jedi -e rebels /etc/group # Looking for existing groups
$ sudo groupadd jedi
$ sudo groupadd rebels
```

2. Create the following user accounts with default home directories and login shell (for example account luke should have home directory /home/luke and a bash shell).

> What option do you need to specify to have useradd create a home directory?

We need to add the flag -m.

> What is the default login shell for users created with useradd ? What command should we use to change the default login shell from /bin/sh to /bin/bash ?

The command useradd uses as default login shell a shell defined in /etc/default/useradd specified by the SHELL variables. By default, we have /bin/sh. We can change the login shell with the flag -s /bin/bash to change the login shell with /bin/bash.

Before creating them verify that they do not yet exist.

> Account luke , assigned to groups jedi (principal) and rebels .

```
$ grep -e luke -e vader -e solo /etc/passwd # Looking for existing groups
$ sudo useradd -g jedi -G rebels -m -s /bin/bash luke
```

> Account vader , assigned to group jedi (principal).

```
$ sudo useradd -g jedi -m -s /bin/bash vader
```

> Account solo , assigned to group rebels (principal).

```
$ sudo useradd -g rebels -m -s /bin/bash solo
```

3. Set a password for the account luke .

```
$ sudo passwd luke
```

4. Test the account luke . Verify that the user can log in and create files. Verify that the user cannot access sensitive system information such as the file /etc/shadow .

```
vpeer@VINCENT-PC:/$ su luke
Password:
luke@VINCENT-PC:/$ cd /home/luke
luke@VINCENT-PC:/$ echo "create new file" > file
luke@VINCENT-PC:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
```

5. Use su to change your account to that of vader . Test if the user vader has access to the files in the home directory of user luke .

```
luke@VINCENT-PC:/$ su vader
Password:
vader@VINCENT-PC:/$ cd home/luke/
vader@VINCENT-PC:/home/luke$ cat file
create new file
```

Task 2: Change group membership

> Create the account leia without assigning it a principal group. After it was created, which principal group did it get assigned?

```
$ sudo useradd leia
$ id leia
uid=1004(leia) gid=1005(leia) groups=1005(leia)
```

Leia's principal group is leia (the same as her username).

> Make leia member of the group rebels (as secondary group).

```
$ sudo usermod -G rebels leia
$ id leia
uid=1004(leia) gid=1005(leia) groups=1005(leia),1004(rebels)
```

> Make leia leave the group rebels and join the group jedi instead.

```
$ sudo usermod -G jedi leia
$ id leia
uid=1004(leia) gid=1005(leia) groups=1005(leia),1003(jedi)
```

Using the usermod -G feature : [...] If the user is currently a member of a group which is not listed, the user will be removed from the group. [...]

> Make leia leave any secondary group.

```
$ sudo usermod -G "" leia
$ id leia
uid=1004(leia) gid=1005(leia) groups=1005(leia)
```

A strategy found on https://unix.stackexchange.com/questions/29570/how-do-i-remove-a-user-from-a-group

Task 3: Give a user sudo rights

Questions:

a) Which line in /etc/sudoers gives the members of the group sudo the right to execute any command?

```
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

b) How would you have to modify this line so that users can use sudo without typing a password (this is in general not recommended, but can be handy sometimes).

```
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) NOPASSWD: ALL
```

Source: https://linuxtect.com/how-to-run-sudo-command-without-password-with-nopasswd/

> Give the account luke sudo rights.

```
$ sudo usermod -a -G sudo luke
```

> Test the new rights. Verify that luke can read the file /etc/shadow using sudo.

```
luke@VINCENT-PC:~$ sudo cat /etc/shadow
[sudo] password for luke:
root:*:19360:0:99999:7:::
daemon:*:19360:0:99999:7:::
[...]
```

> Remove sudo rights from the account luke.

```
$ sudo deluser luke sudo
Removing user `luke' from group `sudo' ...
Done.
```

Task 4: Remove a user account

1. Remove the account leia , but do not delete the home directory yet.

```
$ sudo userdel leia
```

Leia's account is deleted but her home directory still exsits 2. Inspect the home directory (look at the file metadata). What has changed?

```
$ sudo ls -la /home/leia
total 20
drwxr-x--- 2 1004 1005 4096 May 29 16:14 .
drwxr-xr-x 7 root root 4096 May 29 16:14 ..
-rw-r--r-- 1 1004 1005  220 Jan  6  2022 .bash_logout
```

```
-rw-r--r-- 1 1004 1005 3771 Jan  6  2022 .bashrc
-rw-r--r-- 1 1004 1005  807 Jan  6  2022 .profile
```

Files and folders still exist but the owner is represented now with the UID that Leia had.
3. Suppose the user leia has created other files on the system, but you do not know where they are. How would you systematically scan the whole system to find them?

```
$ sudo find / -uid 1004
```

This command will look from the root for every file where the UID owner is 1004, where 1004 is Leia's ancient uid.
4. Remove the home directory manually.

```
/home$ sudo rm -rf leia
```