ADS - System administration
Prof. Fabien Dutoit
BA6 - 2023-2024

Lab report #7

Account management

Germano Thomas **Martins Alexis** **Saez Pablo**

26.05.2024

Table des matières

1 - Introduction

This laboratory will guide us throughout the management of the account in a UNIX system. We will learn how to create, manage user and delete their account properly.

2 - Task 0: Examine the setup of your own account

2.1 - 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(alexis) gid=1000(alexis) groups=1000(alexis),4(adm),20(dialout),24(cdrom),25(floppy),27
$ ls -lisa /etc/passwd
29543 4 -rw-r--r-- 1 root root 1420 Dec 15 22:05 /etc/passwd
$ ls -lisa /etc/group
29550 4 -rw-r--r-- 1 root root 784 Dec 15 22:05 /etc/group
```

- **UID of the Account:** 1000
- **Principal Group:** alexis
- **GID of the Principal Group:** 1000
- **Other Groups the Account is a Member of:** adm (4), dialout (20), cdrom (24), floppy (25), sudo (27), audio (29), dip (30), video (44), plugdev (46), netdev (116)

2.2 - Which skeleton files have been copied?

```
$ ls -la /etc/skel/
total 20
drwxr-xr-x  2 root root 4096 Nov 22 22:36 .
drwxr-xr-x 73 root root 4096 May 13 19:45 ..
-rw-r--r--  1 root root  220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root root 3771 Jan  6  2022 .bashrc
-rw-r--r--  1 root root  807 Jan  6  2022 .profile
```

3 - Task 1: Create user accounts

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

```
$ getent group jedi
$ getent group rebels
$ sudo groupadd jedi
$ sudo groupadd rebels
$ getent group jedi
jedi:x:1001:
$ getent group rebels
rebels:x:1002:
```

3.2 - 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).

```
$ getent passwd luke || sudo useradd -m -g jedi -G rebels -s /bin/bash luke
$ getent passwd vader || sudo useradd -m -g jedi -s /bin/bash vader
$ getent passwd solo || sudo useradd -m -g rebels -s /bin/bash solo
```

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

If we want to also create the home directory of the user, we should specify the option `-m` or `--create-home`.

```
-m, --create-home             create the user's home directory
```

3.2.2 - 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 default login shell is `/bin/sh` and if we want to change that, we should use the parameter `-s` or `--shell`.

```
-s, --shell SHELL             login shell of the new account
```

3.3 - Set a password for the account luke

```
$ sudo passwd luke
New password:
Retype new password:
passwd: password updated successfully
```

3.4 - 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

```
$ su - luke
Password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 4.19.128-microsoft-standard x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This message is shown once a day. To disable it please create the
/home/luke/.hushlogin file.

$ touch ~/toto.txt

$ ls -l toto.txt
-rw-r--r-- 1 luke jedi 0 May 13 20:47 toto.txt

$ cat /etc/shadow
cat: /etc/shadow: Permission denied
```

3.5 - 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

```
$ su - vader
Password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 4.19.128-microsoft-standard x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This message is shown once a day. To disable it please create the
/home/vader/.hushlogin file.

$ ls -l /home/luke/testfile.txt$
ls: cannot access '/home/luke/testfile.txt$': No such file or directory
```

4 - Task 2: Change group membership

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

```
$ sudo useradd -N -m leia
$ id leia
uid=1004(leia) gid=100(users) groups=100(users)
```

4.2 - Make leia member of the group rebels (as secondary group)

```
$ sudo usermod -a -G rebels leia
$ id leia
uid=1004(leia) gid=100(users) groups=100(users),1002(rebels)
```

4.3 - Make leia leave the group rebels and join the group jedi instead

```
$ sudo gpasswd -d leia rebels
$ sudo usermod -a -G jedi leia
Removing user leia from group rebels
$ id leia
uid=1004(leia) gid=100(users) groups=100(users),1001(jedi)
```

4.4 - Make leia leave any secondary group

```
$ sudo usermod -G "" leia
$ id leia
uid=1004(leia) gid=100(users) groups=100(users)
```

5 - Task 3: Give a user sudo rights

5.1 - 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
```

5.2 - 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
```

5.3 - Perform the following steps and give in the lab report the commands you used

5.3.1 - Give the account luke sudo rights

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

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

```
$ su - luke
Password:

luke@... $ sudo cat /etc/shadow
[sudo] password for luke:
root:*:19683:0:99999:7:::
daemon:*:19683:0:99999:7:::
bin:*:19683:0:99999:7:::
sys:*:19683:0:99999:7:::
 ...
```

5.3.3 - Remove sudo rights from the account luke

```
$ sudo gpasswd -d luke sudo
Removing user luke from group sudo

$ su - luke
Password:

luke@... $ sudo cat /etc/shadow
luke is not in the sudoers file.  This incident will be reported.
```

6 - Task 4: Remove a user account

6.1 - Remove the account leia , but do not delete the home directory yet

```
$ sudo userdel leia
$ ls /home/
alexis  leia  luke  solo  vader
```

6.2 - Inspect the home directory (look at the file metadata). What has changed?

```
$ ls -lisa /home/leia/
sudo ls -lisa /home/leia/
total 20
29586 4 drwxr-x--- 2 1004 users 4096 May 13 21:09 .
16386 4 drwxr-xr-x 7 root root  4096 May 13 21:09 ..
29588 4 -rw-r--r-- 1 1004 users  220 Jan  6  2022 .bash_logout
29589 4 -rw-r--r-- 1 1004 users 3771 Jan  6  2022 .bashrc
29587 4 -rw-r--r-- 1 1004 users  807 Jan  6  2022 .profile
```

The name of `leia` has been replaced with its UID. This is because the UID is not recognize by the system anymore.

6.3 - 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 / -user 1004 2>/dev/null
/home/leia
/home/leia/.profile
/home/leia/.bash_logout
/home/leia/.bashrc
 ...
```

6.4 - Remove the home directory manually

```
$ sudo rm -r /home/leia
$ ls /home/
alexis  luke  solo  vader
```

7 - Conclusion

In this laboratory, we really learned how to manage users throughout the whole lifecycle of their account. This could be useful if one day we have manage account in our company. We can imagine combining that with the scripting part we have learn before, so we can automatize the whole process.