EPAM University Programs
DevOps external course
Module 4 Linux & Bash Essentials
TASK 4.6

1. *User management*. Here we suppose there are at least two users, namely, root and guest.
(i) Create a new user *user*
groupadd user
useradd -g user -s /bin/bash -d /home/user -m user
passwd user
id user
ls -ld /home/user
(ii) Log in to the system as “user” (hint use **su**).

```
Last login: Mon Mar  9 09:12:54 2020 from 85.198.133.150
[centos@ip-172-31-42-71 ~]$ groupadd user
groupadd: Permission denied.
groupadd: cannot lock /etc/group; try again later.
[centos@ip-172-31-42-71 ~]$ sudo groupadd user
[centos@ip-172-31-42-71 ~]$ sudo useradd -g user -s /bin/bash -d /home/user -m user
[centos@ip-172-31-42-71 ~]$ passwd user
passwd: Only root can specify a user name.
[centos@ip-172-31-42-71 ~]$ sudo passwd user
Changing password for user user.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[centos@ip-172-31-42-71 ~]$ id user
uid=1001(user) gid=1001(user) groups=1001(user)
[centos@ip-172-31-42-71 ~]$ ls -ld /home/user
drwx------ 2 user user 62 Apr 23 11:06 /home/user
[centos@ip-172-31-42-71 ~]$ sudo su user
[user@ip-172-31-42-71 centos]$
```

(ii) Edit **/etc/passwd** to prevent user *user* from logging in to the system.

2. *Content of* **/etc/passwd** and **/etc/group**.

```
[centos@ip-172-31-42-71 ~]$ sudo passwd -l user
Locking password for user user.
passwd: Success
[centos@ip-172-31-42-71 ~]$ cat /etc/passwd | grep user
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
user:x:1001:1001::/home/user:/bin/bash
[centos@ip-172-31-42-71 ~]$
```

(i) Look through **/etc/passwd** and **/etc/group** (hint: use **less** or **cat**).
(ii) Get data from **/etc/passwd** and **/etc/group** about users: *root*, *guest*, *user* (hint: filter by **grep**).

```
[centos@ip-172-31-42-71 ~]$ echo passwd; sudo cat /etc/passwd | grep 'user\|root\|guest'; echo 'group'; cat /etc/group | grep 'user\|root\|guest'
passwd
root:x:0:0:root:/root:/bin/bash
operator:x:11:0:operator:/root:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
user:x:1001:1001::/home/user:/bin/bash
group
root:x:0:
users:x:100:
rpcuser:x:29:
user:x:1001:
[centos@ip-172-31-42-71 ~]$
```

(iii)Parse **/etc/passwd** and **/etc/group** with cut.

cut -f1 -d: /etc/passwd

```
[centos@ip-172-31-42-71 ~]$ cut -f1 -d: /etc/passwd
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
operator
games
ftp
nobody
systemd-network
dbus
polkitd
rpc
rpcuser
nfsnobody
sshd
postfix
chrony
centos
user
```

cut -f1,2 -d: /etc/passwd

```
[centos@ip-172-31-42-71 ~]$ cut -f1,2 -d: /etc/pass
root:x
bin:x
daemon:x
adm:x
lp:x
sync:x
shutdown:x
halt:x
mail:x
operator:x
games:x
ftp:x
nobody:x
systemd-network:x
dbus:x
polkitd:x
rpc:x
rpcuser:x
nfsnobody:x
sshd:x
postfix:x
chrony:x
centos:x
user:x
```

cut -f1,7 -d: /etc/passwd

```
[centos@ip-172-31-42-71 ~]$ cut -f1,7 -d: /etc/passwd
root:/bin/bash
bin:/sbin/nologin
daemon:/sbin/nologin
adm:/sbin/nologin
lp:/sbin/nologin
sync:/bin/sync
shutdown:/sbin/shutdown
halt:/sbin/halt
mail:/sbin/nologin
operator:/sbin/nologin
games:/sbin/nologin
ftp:/sbin/nologin
nobody:/sbin/nologin
systemd-network:/sbin/nologin
dbus:/sbin/nologin
polkitd:/sbin/nologin
rpc:/sbin/nologin
rpcuser:/sbin/nologin
nfsnobody:/sbin/nologin
sshd:/sbin/nologin
postfix:/sbin/nologin
chrony:/sbin/nologin
centos:/bin/bash
user:/bin/bash
```

cut -f1 -d: /etc/group

```
[centos@ip-172-31-42-71 ~]$ cut -f1 -d: /etc/group
root
bin
daemon
sys
adm
tty
disk
lp
mem
kmem
wheel
cdrom
mail
man
dialout
floppy
games
tape
video
ftp
lock
audio
nobody
users
utmp
utempter
input
systemd-journal
systemd-network
dbus
polkitd
rpc
ssh_keys
cgred
rpcuser
nfsnobody
sshd
postdrop
postfix
chrony
centos
user
```

cut -f1,2 -d: /etc/group

```
[centos@ip-172-31-42-71 ~]$ cut -f1,2 -d: /etc/group
root:x
bin:x
daemon:x
sys:x
adm:x
tty:x
disk:x
lp:x
mem:x
kmem:x
wheel:x
cdrom:x
mail:x
man:x
dialout:x
floppy:x
games:x
tape:x
video:x
ftp:x
lock:x
audio:x
nobody:x
users:x
utmp:x
utempter:x
input:x
systemd-journal:x
systemd-network:x
dbus:x
polkitd:x
rpc:x
ssh_keys:x
cgred:x
rpcuser:x
nfsnobody:x
sshd:x
postdrop:x
postfix:x
chrony:x
centos:x
user:x
```

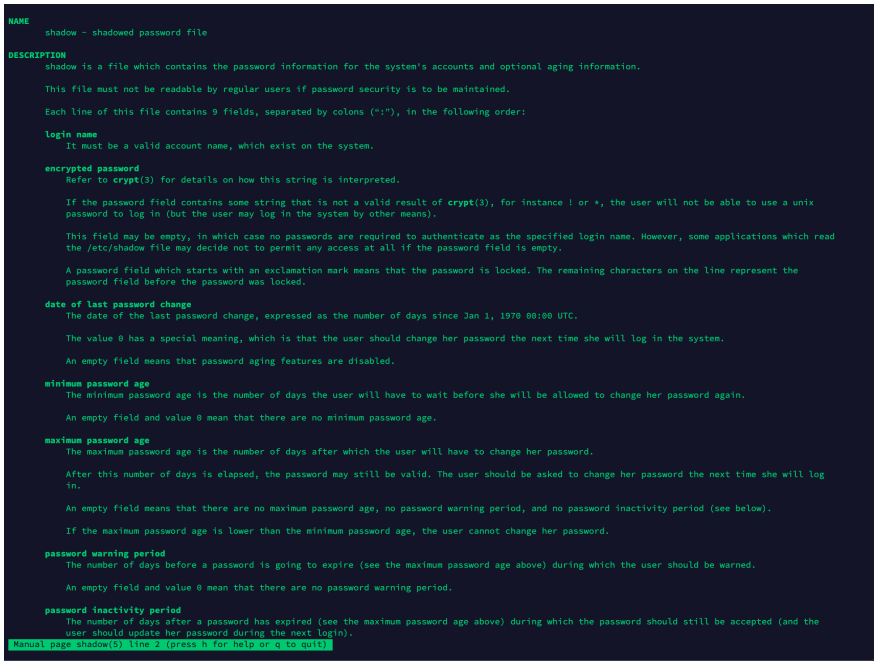
(iv) Try to call **less** on **/etc/shadow** and invoke
sudo less /etc/shadow

```
root:!!:17924:0:99999:7:::
bin:*:17834:0:99999:7:::
daemon:*:17834:0:99999:7:::
adm:*:17834:0:99999:7:::
lp:*:17834:0:99999:7:::
sync:*:17834:0:99999:7:::
shutdown:*:17834:0:99999:7:::
halt:*:17834:0:99999:7:::
mail:*:17834:0:99999:7:::
operator:*:17834:0:99999:7:::
games:*:17834:0:99999:7:::
ftp:*:17834:0:99999:7:::
nobody:*:17834:0:99999:7:::
systemd-network:!!:17924::::::
dbus:!!:17924::::::
polkitd:!!:17924::::::
rpc:!!:17924:0:99999:7:::
rpcuser:!!:17924::::::
nfsnobody:!!:17924::::::
sshd:!!:17924::::::
postfix:!!:17924::::::
chrony:!!:17924::::::
centos:!!:18328:0:99999:7:::
user:!!$6$PO4lBQGk$9KoVSa.EsUtLXaDZya.hjwbGE/IOgtYl/vylH4T/X802SCnlmNSr4Rd7MoNMd6dj5KU9bfpW5xjgkkTySb.z5/:18375:0:99999:7:::
/etc/shadow (END)
```

man -k shadow

```
[centos@ip-172-31-42-71 ~]$ man -k shadow
gpasswd (1)          - administer /etc/group and /etc/gshadow
grpconv (8)          - convert to and from shadow passwords and groups
grpunconv (8)        - convert to and from shadow passwords and groups
gshadow (5)          - shadowed group file
login.defs (5)       - shadow password suite configuration
pwconv (8)           - convert to and from shadow passwords and groups
pwhistory_helper (8) - Helper binary that transfers password hashes from passwd or shadow to opasswd
pwunconv (8)         - convert to and from shadow passwords and groups
shadow (3)           - encrypted password file routines
shadow (5)           - shadowed password file
vigr (8)             - edit the password, group, shadow-password or shadow-group file
vipw (8)             - edit the password, group, shadow-password or shadow-group file
[centos@ip-172-31-42-71 ~]$
```

man 5 shadow



```
NAME
       shadow - shadowed password file

DESCRIPTION
       shadow is a file which contains the password information for the system's accounts and optional aging information.

       This file must not be readable by regular users if password security is to be maintained.

       Each line of this file contains 9 fields, separated by colons (":"), in the following order:

       login name
           It must be a valid account name, which exist on the system.

       encrypted password
           Refer to crypt(3) for details on how this string is interpreted.

           If the password field contains some string that is not a valid result of crypt(3), for instance ! or *, the user will not be able to use a unix
           password to log in (but the user may log in the system by other means).

           This field may be empty, in which case no passwords are required to authenticate as the specified login name. However, some applications which read
           the /etc/shadow file may decide not to permit any access at all if the password field is empty.

           A password field which starts with an exclamation mark means that the password is locked. The remaining characters on the line represent the
           password field before the password was locked.

       date of last password change
           The date of the last password change, expressed as the number of days since Jan 1, 1970 00:00 UTC.

           The value 0 has a special meaning, which is that the user should change her password the next time she will log in the system.

           An empty field means that password aging features are disabled.

       minimum password age
           The minimum password age is the number of days the user will have to wait before she will be allowed to change her password again.

           An empty field and value 0 mean that there are no minimum password age.

       maximum password age
           The maximum password age is the number of days after which the user will have to change her password.

           After this number of days is elapsed, the password may still be valid. The user should be asked to change her password the next time she will log
           in.

           An empty field means that there are no maximum password age, no password warning period, and no password inactivity period (see below).

           If the maximum password age is lower than the minimum password age, the user cannot change her password.

       password warning period
           The number of days before a password is going to expire (see the maximum password age above) during which the user should be warned.

           An empty field and value 0 mean that there are no password warning period.

       password inactivity period
           The number of days after a password has expired (see the maximum password age above) during which the password should still be accepted (and the
           user should update her password during the next login).
Manual page shadow(5) line 2 (press h for help or q to quit)
```

Analyse content of **/etc/shadow** based on what you've found in **man** 5 shadow.
shadow — is a file which contains the password information for the system's accounts and optional aging information.
/etc/shadow — Secure user account information.
Each line of this file contains 9 fields, separated by colons (":"), in the following order: login name, 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 example **user:!!6PO4lBQGk$9KoVSa.EsUtLXaDZya.hjwbGE/lOgtYl/vylH4T/X802SCnlmNSr4Rd7MoNMd6dj5KU9bfpW5xjgkkTySb.z5/:18375:0:99999:7:::**

3. Dealing with **chmod**.

(i) An executable script. Open your favourite editor and put these lines into a file

#!/bin/bash

echo “Drugs are bad MKAY?”

Give name “script.sh” to the script and call to

chmod +x script.sh

Then you are ready to execute the script:

./**script.sh**

```
[centos@ip-172-31-42-71 ~]$ mcedit script

[centos@ip-172-31-42-71 ~]$ mv script script.sh
[centos@ip-172-31-42-71 ~]$ cat
ls
ls
^C
[centos@ip-172-31-42-71 ~]$ ls
script.sh
[centos@ip-172-31-42-71 ~]$ chmod +x script.sh
[centos@ip-172-31-42-71 ~]$ ./script.sh
“Drugs are bad MKAY?”
[centos@ip-172-31-42-71 ~]$
```

(ii) Suppose, you have logged in to the system as *guest*. Create directory “testDir” in the **/tmp**; put some file into testDir and prohibit user *user* from visiting this directory (i.e. “testDir”).

```
[centos@ip-172-31-42-71 ~]$ sudo chown root:root /tmp/testDir/
[centos@ip-172-31-42-71 ~]$ sudo chown -R root:root /tmp/testDir/
[centos@ip-172-31-42-71 ~]$ sudo su user
[user@ip-172-31-42-71 centos]$ ls -la /tmp/testDir/
total 8
drwxrwxr-x   2 root root   27 Apr 23 15:43 .
drwxrwxrwt. 10 root root  204 Apr 23 15:42 ..
-rw-------   1 root root 5027 Apr 23 15:43 .bash_history
[user@ip-172-31-42-71 centos]$ Last login: Thu Apr 23 15:42:18 2020 from 46.98.128.86
[centos@ip-172-31-42-71 ~]$ ls -la /tmp/testDir/
total 8
drwxrwxr-x   2 root root   27 Apr 23 15:43 .
drwxrwxrwt. 10 root root  204 Apr 23 15:59 ..
-rw-------   1 root root 5027 Apr 23 15:43 .bash_history
[centos@ip-172-31-42-71 ~]$ sudo chmod 700 -R /tmp/testDir/
[centos@ip-172-31-42-71 ~]$ ls -la /tmp/testDir/
ls: cannot open directory /tmp/testDir/: Permission denied
[centos@ip-172-31-42-71 ~]$ sudo ls -la /tmp/testDir/
total 8
drwx------   2 root root   27 Apr 23 15:43 .
drwxrwxrwt. 10 root root  204 Apr 23 15:59 ..
-rwx------   1 root root 5027 Apr 23 15:43 .bash_history
[centos@ip-172-31-42-71 ~]$ sudo su user
[user@ip-172-31-42-71 centos]$ cd /tmp/
.font-unix/                                                    testDir/
.ICE-unix/                                                     .Test-unix/
mc-centos/                                                     .X11-unix/
systemd-private-3b692bc9a1c9440e808a6f3087e3ddb0-chronyd.service-dG0HGQ/ .XIM-unix/
[user@ip-172-31-42-71 centos]$ cd /tmp/testDir/
bash: cd: /tmp/testDir/: Permission denied
[user@ip-172-31-42-71 centos]$
```

(iii) Test, if it possible to forbid an owner of some file to read to or write from this file.

```
[centos@ip-172-31-42-71 ~]$ sudo chmod u-rw -R /tmp/testDir/
[centos@ip-172-31-42-71 ~]$ sudo ls -la /tmp/testDir/
total 8
d--x------   2 root root   27 Apr 23 15:43 .
drwxrwxrwt. 10 root root  204 Apr 23 16:26 ..
---x------   1 root root 5027 Apr 23 15:43 .bash_history
```